21 世纪计算机系列规划教材

# 计算机网络基础与实训

主编　周观民　王东霞

電子工業出版社

**Publishing House of Electronics Industry**

北京・BEIJING

## 内 容 简 介

本书层次清楚，概念准确，深入浅出，语言通俗易懂。全书坚持“实用为主，强化职业能力”的原则，侧重理论联系实际，结合高等职业院校学生的特点注重基本能力和基本技能的培养。

本书全面介绍计算机网络基础知识、网络体系结构与网络标准、网络互联技术、网络规划与设计、网络安全等基础理论知识，并在此基础上介绍了网络工程应用开发过程以及用 Windows Server 2003 为服务器组建 Internet 典型应用环境。

本书既可以作为高职高专计算机、电子、电子商务和机电等专业的计算机网络基础课程教材；亦可作为高职高专其他各非电子类专业的计算机网络基础教材；还可作为各类计算机网络培训教材，以及从事计算机网络设计与应用的技术人员或计算机网络爱好者的参考书。



**图书在版编目（CIP）数据**

计算机网络基础与实训 / 周观民，王东霞主编. —北京：电子工业出版社，2011.9
21 世纪计算机系列规划教材
ISBN 978-7-121-14288-8

Ⅰ. ①计… Ⅱ. ①周… ②王… Ⅲ. ①计算机网络－高等职业教育－教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2011)第 158771 号

策划编辑：柴　灿
责任编辑：郝黎明　　文字编辑：裴　杰
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：16.5　字数：422.4 千字
印　　次：2011 年 9 月第 1 次印刷
印　　数：3 000 册　　定价：30.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

“计算机网络基础与实训”是按照高职高专学生培养目标和基本要求，并结合作者多年的教学和工程实践经验，编写的一本计算机网络技术基础与实训教材。

本书特色如下：

在组织方式上，按照学习领域的课程改革思路进行教材的组织编写，坚持实用技术和工程实践相结合的原则。

在目标上，以适应高职高专教学改革的需要为目标，充分体现高职特色，有所创新和突破，全书按照学生获得网络能力递进的阶段，精选了 11 个实验。

在内容选取上，坚持集先进性、科学性和实用性为一体，尽可能选取最新、最实用的技术与当前企业实际需要的网络技术接轨。

在教材内容深浅程度上，把握理论够用、侧重实践、由浅入深的原则，以使学生分层分步骤掌握所学的知识。

在教材结构上，全书共分为 9 章：第 1 章，计算机网络概述；第 2 章，数据通信基础；第 3 章，计算机网络体系结构；第 4 章，局域网技术；第 5 章，Internet 应用基础；第 6 章，网络操作系统；第 7 章，网络规划设计与综合布线；第 8 章，网络管理与安全；第 9 章，基础实验与综合实训指导。

本书由周观民，王东霞担任主编，参加编写的人员还有：魏金太、周颖琦、张延玲、赵松林和邓续方。在本书的编写过程中，得到了河南省教育厅职业教育教研室的大力支持，在此表示衷心感谢！

编者意在奉献给读者一本实用并具有特色的教材，但由于书中涉及的许多内容属于正在发展中的高新技术，加之我们水平有限，难免有错误和不妥之处，敬请广大读者给予批评指正。E-mail:zhougm@jyvtc.edu.cn。

编　者

# 目　　录

# 第 1 章

# 计算机网络概述

目前，人们可以通过多种方式，将自己的个人计算机、PDA 或手机通过电话线、网络线等有线方式或通过无线移动网等无线方式连接到互联网上，以此来享受互联网所提供的各种各样的服务，如浏览 Web 页面、远程上传与下载文件、发送或接收电子邮件、网上实时交谈、网络游戏等。计算机网络已经无处不在，网络正在改变我们的生活。

本章从计算机网络的产生与发展入手，介绍计算机网络的概念、常用的网络拓扑结构、网络操作系统及计算机网络的标准和标准化组织等内容。

通过本章的学习，应达到如下学习目标：

（1）了解计算机网络的产生与发展过程；

（2）熟悉计算机网络的定义、构成、功能和分类；

（3）了解计算机网络拓扑结构的概念，熟悉常见的拓扑结构及其特点；

（4）了解网络操作系统的概念、功能及分类，熟悉常见的网络操作系统的特点；

（5）了解计算机网络的标准。

## 1.1 计算机网络的产生与发展

### 1.1.1 计算机网络的发展简史

计算机网络是计算机技术与通信技术相结合的产物。通信网为计算机网络提供了便利而广泛的信息传输通道，而计算机和计算机网络技术的发展也促进了通信技术的发展。计算机网络从形成、发展到广泛应用已经历了几十年的时间。

1946 年诞生的世界上第一台电子数字计算机，开创了向信息社会迈进的新纪元。20 世纪 50 年代，美国利用计算机技术建立了半自动化的地面防空系统（SAGE），它将雷达信息和其他信号经远程通信线路传送至计算机进行处理，第一次利用计算机网络实现远程集中控制，这是计算机网络的雏形。

随着计算机技术和通信技术的不断发展，计算机网络也经历了从简单到复杂、从单机到多机，由终端与计算机之间的通信演变到计算机与计算机之间的直接通信的发展过程，其发展过程大致可分为远程联机、多机互联网络、标准、开放的计算机网络和高速、智能的计算机网络 4 个阶段。

### 1．远程联机阶段

计算机诞生后的很长时间内，一台价值不菲的计算机只能供单用户独占使用，为了共享主机资源和信息采集以及综合处理，用一台计算机通过通信线路与多台用户终端相连，用户通过终端命令以交互方式使用计算机，人们把它称为远程联机系统。

远程联机系统的特点是系统中只有一个计算机处理中心，各终端通过通信线路共享主计算机的硬件和软件资源，终端不具备自主处理的功能，主计算机既要承担数据处理又要承担与各终端之间的通信工作，因此，主计算机负担过重，终端独占线路，资源利用率低。此阶段也可称为“终端—计算机”网络，如图 1-1 所示的远程联机。

### 2．多机互联网络阶段

20 世纪 60 年代中期至 70 年代中期，随着计算机技术和通信技术的发展，将多个远程联机系统终端网络互相连接起来，形成“计算机—计算机”网络，实现了更广范围内的资源共享。网络中各个计算机系统相互独立，依靠通信线路进行交换信息，通信方式为计算机和计算机之间的通信。计算机网络要完成数据处理与数据通信两大基本功能，因此在逻辑结构上可以将其分成资源子网和通信子网两部分。资源子网的任务是负责全网的信息处理，通信子网将各种计算机互连起来完成数据传输、交换和通信处理。

这一阶段结构上的主要特点是：以通信子网为中心，多主机多终端。1969 年在美国建成的 ARPANET 是这一阶段的代表。在 ARPANET 上首先实现了以资源共享为目的不同计算机互连的网络，它奠定了计算机网络技术的基础，成为今天 Internet 的前身。

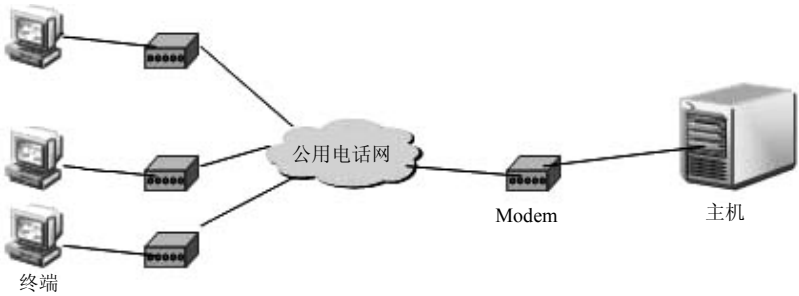



图 1-1　远程联机

### 3．标准、开放的计算机网络阶段

20 世纪 70 年代，计算机网络大都采用直接通信方式。1972 年后，以太网 LAN、MAN、WAN 迅速发展，各个计算机生产商纷纷发展各自的网络系统，制定自己的网络技术标准。1974 年，IBM 公司公布了它研制的系统网络体系结构。随后 DGE 公司宣布了自己的数字网络体系结构，1976 年 UNIVAC 宣布了该公司的分布式通信体系结构。这个时期，虽然不断出现的各种网络极大地推动了计算机网络的应用，但是众多不同的专用网络体系标准给不同网络间的互连带来了很大的不便。鉴于这种情况，国际标准化组织（ISO）于 1977 年成立了专门的机构从事“开放系统互连”问题的研究，目的是设计一个标准的网络体系模型。1984 年 ISO 颁布了“开放系统互连基本参考模型”，这个模型通常被称作 OSI 参考模型。只有标准的才是开放的，OSI 参考模型的提出引导着计算机网络走向开放的标准化的道路，同时也标志着计算机网络的发展步入了成熟的阶段。

**4．高速、智能的计算机网络阶段**

近年来，随着通信技术，尤其是光纤通信技术的发展，计算机网络技术得到了迅猛的发展。光纤作为一种高速率、高带宽、高可靠性的传输介质，在各国的信息基础建设中使用越来越广泛，这为建立高速的网络铺垫了基础。千兆位乃至万兆位传输速率的以太网已经被越来越多地用于局域网和城域网中，而基于光纤的广域网链路的主干带宽也已达到 10Gbps 数量级。网络带宽的不断提高，更加刺激了网络应用的多样化和复杂化，多媒体应用在计算机网络中所占的份额越来越高。同时，用户不仅对网络的传输带宽提出越来越高的要求，对网络的可靠性、安全性和可用性等也提出了新的要求。为了向用户提供更高的网络服务质量，网络管理也逐渐进入了智能化阶段，包括网络的配置管理、故障管理、计费管理、性能管理和安全管理等在内的网络管理任务都可以通过智能化程度很高的网络管理软件来实现。目前，全球以 Internet 为核心的高速计算机互联网络已经形成，计算机网络已经进入了高速、智能化的发展阶段。

### 1.1.2　计算机网络的发展趋势

未来计算机网络的发展有以下几种基本的技术趋势：

（1）向分布式计算机方向发展；

（2）向适应多媒体通信、移动通信的结构发展；

（3）向智能化及贴近应用的智能化方向发展；

（4）向可靠性更高，服务质量更优，费用更低的方向发展。

## 1.2　计算机网络的基本概念

### 1.2.1　计算机网络的定义

到目前为止，计算机网络并没有一个确切的定义。我们可以简单地描述为：计算机网络是通过通信线路连接起来的自治的计算机集合，以实现资源共享。不难看出该描述包括了 3 个方面的含义：

① 必须有两台或两台以上、具有独立功能的计算机系统相互连接起来，以达到共享资源为目的；

② 计算机互相通信交换信息，必须有一条通道。这条通道的连接是物理的，由物理介质来实现（例如铜线、光纤、微波、卫星等）；

③ 计算机系统之间的信息交换，必须要遵守某种约定和规则。

以上从 3 个方面概括了计算机网络的基本内涵。因此，可以把计算机网络定义为：计算机网络是把分布在不同地点，并具有独立功能的多个计算机系统通过通信设备和线路连接起来，在功能完善的网络软件和协议的管理下，以实现网络中资源共享为目标的系统。

由多台计算机组成的计算机网络系统模型如图 1-2 所示。

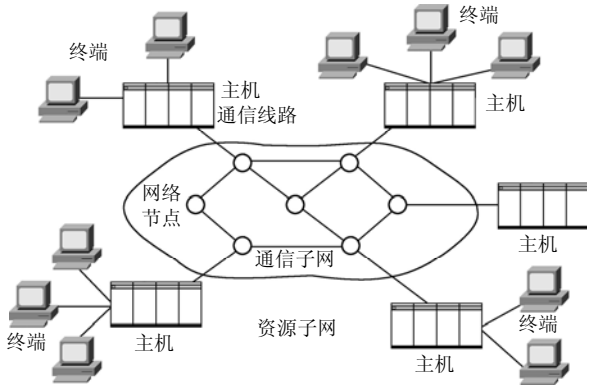



图 1-2　多台计算机组成的计算机网络系统模型

## 1.2.2　计算机网络的构成

从资源构成的角度讲，计算机网络是由硬件和软件组成的。硬件包括各种主机、终端等用户端设备，以及交换机、路由器等通信控制处理设备；软件则由各种系统程序和应用程序以及大量的数据资源组成，包括网络操作系统、网络协议软件、网络管理软件、网络通信软件和网络应用软件等。

从功能上将计算机网络逻辑划分为资源子网和通信子网。其中，资源子网负责全网的数据处理业务，并向网络用户提供各种网络资源和网络服务。资源子网主要由主机、终端以及相应的 I/O 设备、各种软件资源和数据资源构成。主机（HOST）可以是大型机、中型机、小型机、工作站或微型机，它通过高速通信线路与通信控制处理机相连。主机系统拥有各种终端用户要访问的资源，它负担着数据处理的任务。终端（Terminal）是用户进行网络操作时所使用的末端设备，它是用户访问网络的界面。终端设备的种类很多，如电传打字机、CRT 监视器加键盘，另外还有网络打印机、传真机等。终端设备可以直接或者通过通信控制处理机和主机相连。而通信子网的作用则是为资源子网提供传输、交换数据信息的能力。通信子网主要由通信控制处理机、通信链路及其他设备（如调制解调器等）组成。通信链路是用于传输信息的物理信道以及为达到有效、可靠的传输质量所需的信道设备的总称。通常情况下，通信子网中的链路属于高速线路，所用的信道类型可以是有线信道或无线信道。

## 1.2.3　计算机网络的功能

计算机网络技术使计算机的作用范围和其自身的功能有了突破性的发展。计算机网络虽然各种各样，但作为计算机网络都应具有如下功能。

### 1．数据通信

数据通信是计算机网络最基本的功能之一，利用这一功能，分散在不同地理位置的计算机就可以相互传输信息。该功能是计算机网络实现其他功能的基础，如 E-mail、远程数据交换等。

**2．计算机系统的资源共享**

对于用户所在站点的计算机而言，无论硬件或是软件，性能总是有限的。一台个人计算机用户，可以通过使用网络中的某一台高性能的计算机来处理自己提交的某个大型复杂的问题，用户还可以像使用自己的个人计算机一样，使用网上的一台高速打印机打印报表、文档等。更重要的资源是计算机软件和各种各样的数据库，用户可以使用网上的大容量磁盘存储器存放自己采集、加工的信息，特别是可以使用网上已有的软件来解决某个问题。各种各样的数据库更是取之不尽。随着计算机网络覆盖区域的扩大，信息交流已越来越不受地理位置、时间的限制，使得人类对资源可以互通有无，大大提高了资源的利用率和信息的处理能力。

**3．进行数据信息的集中和综合处理**

将分散在各地计算机中的数据资料适时集中或分级管理，并经综合处理后形成各种报表，提供给管理者或决策者分析和参考，如自动订票系统、政府部门的计划统计系统、银行财政及各种金融系统、数据的收集和处理系统、地震资料收集与处理系统、地质资料采集与处理系统等。

**4．均衡负载，相互协作**

当某一台计算中心的任务很重时，可以通过网络将此任务传递给空闲的计算机去处理，以调节忙闲不均现象。此外，地球上不同区域的时差也为计算机网络带来很大的灵活性，一般白天计算机负载较重，晚上则负载较轻，地球时差正好为我们提供了半个地球的调节余地。

**5．提高了系统的可靠性和可用性**

当网络中的某一处理机发生故障时，可由别的路径传输信息或转到别的系统中代为处理，以保证用户的正常操作，不会因为局部故障而导致系统的瘫痪。又如某一数据库中的数据因处理机发生故障而消失或遭到破坏时，可从另一台计算机的备份数据库中调来进行处理，并恢复遭破坏的数据库，从而提高系统的可靠性和可用性。

**6．实现分布式处理**

对于综合性的大型问题可采用合适的算法，将任务分散到网络中不同的计算机上进行分布式处理。特别是对当前流行的局域网更有意义，利用网络技术将微机连成高性能的分布式计算机系统，使它具有解决复杂问题的能力。

以上只是列举了一些计算机网络的常用功能，随着计算机技术的不断发展，计算机网络的功能和提供的服务将会不断增加。

## 1.2.4　计算机网络的类型

由于计算机网络自身的特点，其分类方法有很多种。根据不同的分类原则，可以得到不同类型的计算机网络。

**1．按网络的覆盖范围划分**

根据计算机网络所覆盖的地理范围，计算机网络通常被分为局域网（LAN）、城域网

（MAN）、广域网（WAN）、接入网（AN）。这种分类方法也是目前较为流行的一种分类方法。

（1）局域网（Local Area Network，LAN）

局域网也称局部网，是指将有限的地理区域内的各种通信设备互连在一起的通信网络。它具有很高的传输速率（几十至上吉比特每秒），其覆盖范围一般不超过几十千米，通常将一座大楼或一个校园内分散的计算机连接起来构成 LAN。

（2）城域网（Metropolitan Area Network，MAN）

城域网有时又称为城市网、区域网、都市网。城域网介于局域网（LAN）和广域网（WAN）之间，其覆盖范围通常为一个城市或地区，距离从几十千米到上百千米。城域网中可包含若干个彼此互连的局域网，可以采用不同的系统硬件、软件和通信传输介质构成，从而使不同类型的局域网能有效地共享信息资源。城域网通常采用光纤或微波作为网络的主干通道。

（3）广域网（Wide Area Network，WAN）

广域网指的是实现计算机远距离连接的计算机网络，可以把众多的城域网、局域网连接起来，也可以把全球的区域网、局域网连接起来。广域网涉及的范围较大，一般从几百千米到几万千米，用于通信的传输装置和介质一般由电信部门提供，能实现大范围内的资源共享。

#### 2．按通信传输介质划分

按通信传输介质的不同可分为有线网络和无线网络。所谓有线网络，是指采用有形的传输介质，如双绞线、同轴电缆、光纤等组建的网络；而使用微波、红外线和激光等无线传输介质作为通信线路的网络就属于无线网络和卫星网络等。

#### 3．按网络拓扑结构划分

计算机网络的物理连接方式叫做网络的拓扑结构。按照网络的拓扑结构，计算机网络主要分为总线形、星形、环形、网状、树形和环形网络等。

## 1.3　计算机网络的拓扑结构

### 1.3.1　拓扑结构的概念

在计算机网络中，抛开网络中的具体设备，把服务器、工作站等网络单元抽象为“点”，把网络中的电缆、双绞线等传输介质抽象为“线”，以此来研究网络的结构。

计算机网络的拓扑结构就是指计算机网络中的通信线路和节点相互连接的几何排列方法和模式。拓扑结构影响着整个网络的设计、功能、可靠性和通信费用等方面，是决定局域网性能优劣的重要因素之一。

### 1.3.2　几种典型的网络拓扑结构

#### 1．总线形拓扑结构

总线形拓扑结构是指所有节点共享一根传输总线，所有的站点都通过硬件接口连接在这

根传输线上。其优点是结构简单、价格低廉、安装使用方便；缺点是故障诊断和隔离比较困难，如图 1-3 所示。

### 2．星形拓扑结构

星形拓扑结构是符合令牌协议的高速局域网络。它是以中央节点为中心，把若干外围节点连接起来的辐射式互连结构，如图 1-4 所示。

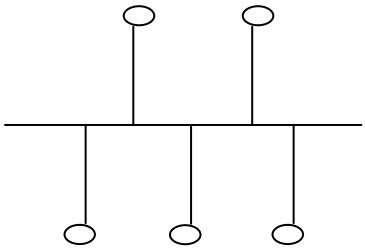


图 1-3　总线形拓扑结构

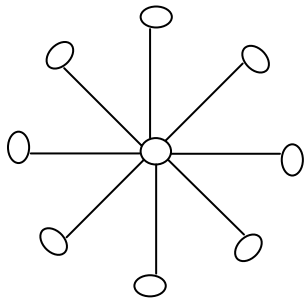


图 1-4　星形拓扑结构

星形拓扑结构的优点是单点故障不影响全网，结构简单。增删节点及维护管理容易；故障隔离和检测容易，延迟时间较短。缺点是成本较高，资源利用率低；网络性能过于依赖中心节点。

### 3．树形拓扑结构

树形拓扑结构是星形结构的扩展，它由根节点和分支节点所构成，如图 1-5 所示。其优点是结构比较简单，成本低。扩充节点方便灵活；缺点是对根的依赖性大。

### 4．环形拓扑结构

环形拓扑结构将所有网络节点通过点到点通信线路连接成闭合环路，数据将沿一个方向逐站传送，每个节点的地位和作用相同，且每个节点都能获得执行控制权，如图 1-6 所示。

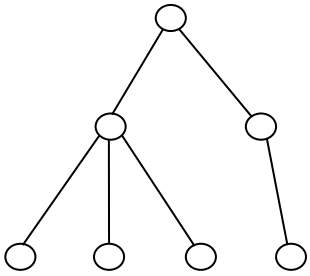


图 1-5　树形拓扑结构

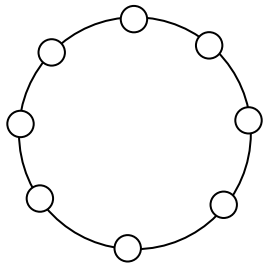


图 1-6　环形拓扑结构

环形结构的显著特点是每个节点用户都与两个相邻节点用户相连。其优点是简化路径选择控制，传输延迟固定，实时性强，可靠性高；缺点是节点过多时，会影响传输效率。环某处断开会导致整个系统的失效，节点的加入和撤出过程复杂。

### 5．网状拓扑结构

网状拓扑结构中的所有节点之间的连接是任意的，没有规律的。实际存在与使用的广域

网基本上都采用网状拓扑结构，如图 1-7 所示。

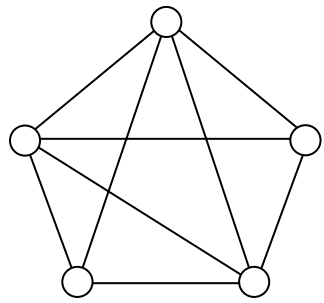


图 1-7　网状拓扑结构

网状拓扑结构的优点是具有较高的可靠性。某一线路或节点有故障时，不会影响整个网络的工作。缺点是结构复杂，需要路由选择和流控制功能，网络控制软件复杂，硬件成本较高，不易管理和维护。

## 1.4　计算机网络的标准及标准化组织

### 1.4.1　计算机网络的标准

计算机网络的标准有合法的标准和既成事实的标准之分。合法的标准就是由一些权威标准化实体采纳的正式的、合法的标准。例如，OSI/RM 就是 ISO 提出的。而既成事实的标准是未曾被相关行业标准化组织认可，但却是广泛应用的标准。例如，Internet 所使用的 TCP/IP，就是即成事实的标准。

### 1.4.2　几个有影响的标准化组织

#### 1．国际标准化组织（ISO）

ISO（International Organization for Standardization）成立于 1946 年，是一个全球性的非政府组织，也是目前世界上最大、最有权威性的国际标准化专门机构。ISO 与 600 多个国际组织保持着协作关系，其主要活动是制定国际标准，协调世界范围的标准化工作，组织各成员国和技术委员会进行情报交流，以及与其他国际组织进行合作，共同研究有关标准化问题。到目前为止，ISO 已制定了 13 736 个国际标准，如著名的具有七层协议结构的开放系统互联参考模型（OSI）、ISO 9000 系列质量管理和品质保证标准等。

#### 2．美国国家标准协会 ANSI

ANSI（American National Standards Institute）是成立于 1918 年的非营利性的民间组织。ANSI 同时也是一些国际标准化组织的主要成员，如国际标准化委员会和国际电工委员会（IEC）。ANSI 标准广泛应用于各个领域，典型应用有：美国标准信息交换码（ASCII）和光

纤分布式数据接口（FDDI）等。

### 3．电气与电子工程师协会 IEEE

IEEE（Institute of Electrical and Electronics Engineers）建会于 1963 年，由从事电气工程、电子和计算机等有关领域的专业人员组成，是世界上最大的专业技术团体。IEEE 是一个跨国的学术组织，目前拥有 36 万会员，近 300 个地区分会分布在 150 多个国家。IEEE 下设许多专业委员会，其定义或开发的标准在工业界有极大的影响和作用力。例如，1980 年成立的 IEEE 802 委员会负责有关局域网标准的制定事宜，制定了著名的 IEEE 802 系列标准，如 IEEE 802.3 以太网标准、IEEE 802.4 令牌总线网标准和 IEEE 802.5 令牌环网标准等。

### 4．国际电信联盟 ITU

1865 年 5 月，由法、德、俄等 20 个国家为了顺利实现国际电报通信，在巴黎成立的一个国际组织“国际电报联盟”；1932 年，70 个国家的代表在西班牙马德里召开会议，“国际电报联盟”改为“国际电信联盟”；1947 年，国际电信联盟成为联合国的一个专门机构。国际电信联盟是电信界最有影响的组织，也是联合国机构中历史最长的一个国际组织，简称“国际电联”或 ITU（International Telecommunication Union）。联合国的任何一个主权国家都可以成为 ITU 的成员。

ITU 是世界各国政府的电信主管部门之间协调电信事务的一个国际组织，它研究制定有关电信业务的规章制度，通过决议提出推荐标准，收集相关信息和情报，其目的和任务是实现国际电信的标准化。

ITU 的实质性工作由无线通信部门（ITU-R）、电信标准化部门（ITU-T）和电信发展部门（ITU-D）承担。其中，ITU-T 就是原来的国际电报电话咨询委员会（CCITT），负责制定电话、电报和数据通信接口等电信标准化。

ITU-T 制定的标准被称为“建议书”，是非强制性的、自愿的协议。由于 ITU-T 标准可保证各国电信网的互连和运转，所以越来越广泛地被世界各国所采用。

### 5．国际电工委员会 IEC

IEC（International Electrotechnical Commission）成立于 1906 年，至今已有近百年的历史，它是世界上成立最早的国际性电工标准化机构，负责有关电气工程和电子工程领域中的国际标准化工作。ISO 正式成立后，IEC 曾作为电工部门并入，但是在技术和财务上仍保持独立性。1979 年 ISO 与 IEC 达成协议：两者在法律上都是独立的组织，IEC 负责有关电气工程和电子工程领域中的国际标准化工作，ISO 则负责其他领域内的国际标准化工作。

### 6．电子工业协会 EIA

EIA（Electronic Industries Association）是美国的一个电子工业制造商组织，成立于 1924 年。EIA 颁布了许多与电信和计算机通信有关的标准。例如，众所周知的 RS-232 标准，定义了数据终端设备和数据通信设备之间的串行连接。这个标准在今天的数据通信设备中被广泛采用。在结构化网络布线领域，EIA 与美国电信行业协会（TIA）联合制定了商用建筑电信布线标准（如 EIA/TIA 568 标准），提供了统一的布线标准并支持多厂商产品和环境。

# 练习 1

## 一、填空题

（1）按覆盖的地理范围分类，计算机网络可以分成_____ 、城域网和_____。

（2）在逻辑上，人们通常将计算机网络分为两个部分，分别称为_____子网和_____子网。

（3）网状拓扑的计算机网络特点是：系统可靠性高，但是_____，必须采用_____和流量控制方法。

## 二、选择题

（1）如果某种局域网的拓扑结构是（　　），则局域网中任何一个节点出现故障都不会影响整个网络的工作。

A．总线形结构　　B．树形结构

C．环形结构　　D．星形结构

（2）在地理上分散布置的多台独立计算机通过通信线路互连构成的系统称为（　　），从而使信息传输与信息功能相结合，使多个用户能够共享软、硬件资源，提高信息的能力。

A．分散系统　　B．电话网

C．计算机网络　　D．智能计算机

## 三、思考题

（1）简述计算机网络的定义、分类和主要功能。

（2）按照网络的逻辑功能可将计算机网络分为哪几部分？各部分的主要功能是什么？

（3）常见的网络拓扑结构有哪几种？试画出它们的网络拓扑结构图并说明各自的特点。

# 第 2 章

# 数据通信基础

计算机网络的主要功能是实现信息资源的共享与交换，而信息是以数据形式来表示的，因此计算机网络首先要从基于数据通信系统之上的资源共享系统这个角度，来解决数据通信的问题。数据通信技术，主要研究数据的传输、交换、存储及处理的理论、方法和技术。

通过本章的学习，应达到如下学习目标：

（1）掌握数据通信的基本概念、相关术语和性能指标；

（2）掌握常用传输介质的类型和特性；

（3）掌握多路复用技术的概念、了解其实现方法；

（4）掌握数据交换技术的概念、了解其实现方法；

（5）了解数据传输中的差错控制技术及常用方法。

## 2.1 相关基本概念

### 2.1.1 数据通信系统的模型

数据通信系统的基本组成有 3 个要素：信源、信宿和信道。图 2-1 所示的是一个简单的数据通信系统模型。

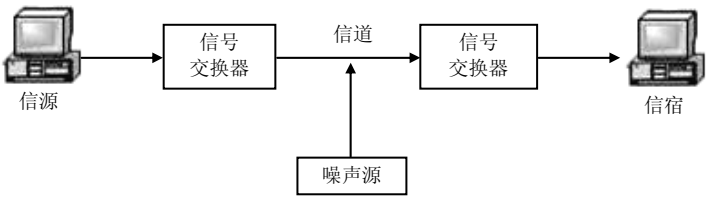



图 2-1 数据通信系统模型

#### 1．信源/信宿

信源是通信过程中产生和发送信息的设备或计算机；信宿是通信过程中接收和处理信息的设备或计算机。信源和信宿是数据的出发点和目的地，又被称为数据终端设备 DTE（Data Terminal Equipment）。通常网络中的多数信息都是双向传输的，因此，信源也可作为信宿，信宿也可作为信源，一个 DTE 通常既是信源又是信宿。

2．信道

信道是指传输信息的通路，一条传输线路上可以存在多个信道。按传输介质的不同可分为有线信道（如双绞线、电缆等）、无线信道（如微波等）和卫星信道等。

3．信号变换器

信号变换器的主要功能是在信源或信宿与信道之间进行信号的变换。如果在模拟信道上传输数字信号，信号变换器采用调制解调器（Modem）；如果在数字信道上传输模拟信号，变换器则采用编码解码器（CODEC）。

4．噪声源

一个通信系统客观上是不可避免地存在着噪声干扰的，而这些干扰分布在数据传输过程中的各个部分。为了分析问题方便，通常把它们等效为一个作用于信道上的噪声源。

## 2.1.2 数据通信的常用术语

1．信息（Information）

信息是人对现实世界事物存在的方式或运动状态的某种认识。通信的目的是信息交换，信息的载体可以是数值、文字、图形、声音、图像和动画等。

2．数据（Data）

数据是运送信息的实体，指描述事物属性的数字、字母或符号等。在通信系统中，数据分为模拟数据和数字数据。模拟数据是指在某个时间间隔中连续变化的值。例如，声音、视频。数字数据是指在某个时间间隔中是离散的值。例如，文本信息和整数等。

3．信号（Signal）

信号是数据在传输过程中电信号的表示形式，有模拟信号和数字信号之分。模拟信号的信号电平是连续变化的，数字信号是指幅度的取值是离散的，幅值表示被限制在有限个数值之内。二进制码就是一种数字信号。二进制码受噪声的影响小，易于数字电路进行处理，所以得到了广泛的应用。按照在传输介质上传输的信号类型，通信系统分为“模拟通信系统”与“数字通信系统”两种。

从上面的表述中可以得出如下结论：数据是信息的载体，信息是数据的内容和解释，而信号是数据的编码。

## 2.1.3 数据通信方式

1．串/并行通信

在数据通信中，如果按同时传输的数据位来划分则可分为串行传输方式和并行传输方式。串行传输方式是指将传送的每个字符的二进制代码按由低位到高位的顺序依次发送，每次只能传输其中的一位；而并行传输方式是将表示字符的多位二进制代码同时通过多条并行通信

信道传送。

在数据通信中，串/并行传输方式最典型的代表就是计算机和网络设备中所见的串行口（COM 口）、并行口（LPT 口）。串行通常用于进行拨号、双机互连通信，并口则常用于打印、游戏等的数据通信。

（1）串行通信

串行通信是指数据在通信线路上一位一位地传送，如图 2-2 所示。由于在计算机内部总线上传输的是并行数据，所以计算机要与外部设备进行串行通信，在发送端就需要把并行数据转换成串行数据，然后逐位地通过通信线路到达接收端，在接收端则需要将串行数据转换成并行数据，以便处理。在网络中，计算机之间也是串行通信，网卡就负责进行串行数据和并行数据的转换工作。

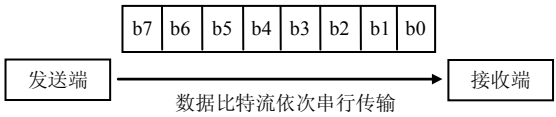



图 2-2　串行通信示意图

（2）并行通信

在并行通信中，一般有多个数据位同时在两台设备之间传输。以 8 位数据位的并行通信为例，如图 2-3 所示。图中发送端和接收端有 8 条数据线相连，发送端同时发送 8 个数据位，接收端同时接收 8 个数据位。计算机内部各部件之间的并行通信是通过总线进行的。微机与并行打印机的通信就是并行通信。

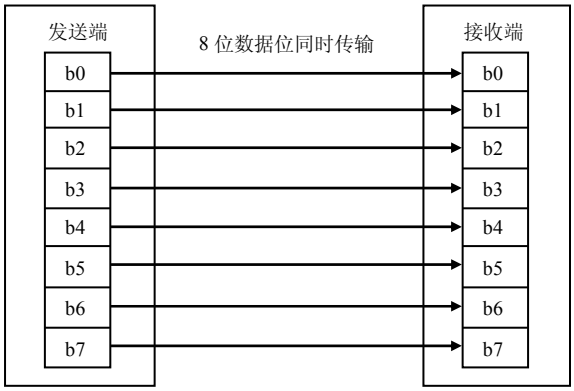



图 2-3　并行通信示意图

从表面上看，并行通信的传输效率要高于串行通信，但这也是有条件的。事实上，因为在并行通信中，同时进行的数据位传输可能存在相互干扰，特别是在传输速率达到一定程度之后。所以并行通信在速率上受到诸多限制，而串行通信却没有这方面的限制，所以现在许多串行通信的传输效率要高于并行通信。在现在诸多的总线技术中，有许多向着串行方式转变，如新兴的高效率总线接口——PCI-E 就是串行传输方式，用来取代原来并行的 PCI；新兴的磁盘 SAS 接口也是串行传输方式，它比并行的 IDE 接口传输效率还高；高速串行接口 USB 也得到了广泛的应用。

### 2．单/双工通信

数据传输按数据流的传送方向可分为单工、半双工通信和全双工通信 3 种传输方式。

（1）单工通信

单工通信指的是两个数据站之间只能沿一个指定的方向进行数据传输，如图 2-4 所示。如数据由 A 端传到 B 端（实线方向），而 B 端至 A 端只传送联络信号（虚线方向）。前者称正向信道，后者称反向信道。一般正向信道传输速率较高，反向信道传输速率较低。此种方式适用于数据收集系统，如气象数据的收集、听广播等就是单工通信的例子。因为在这种数据收集系统中，大量数据只需要从一端到另一端，另外需要少量联络信号通过反向信道传输。


图 2-4　单工通信

（2）半双工通信

半双工通信是两个数据站之间可以在两个方向上进行数据传输，但不能同时进行，如图 2-5 所示。该方式要求 A 端、B 端两端都有发送装置和接收装置。若想改变信息的传输方向，需要由开关 Kl 和 K2 进行切换。如问讯、检索和科学计算等数据通信系统运用的是半双工数据传输。

（3）全双工通信

全双工通信是在两个数据站之间，可以在两个方向同时进行数据传输，如图 2-6 所示。全双工通信效率高，但组成系统的造价高，适用于计算机之间高速数据通信系统。

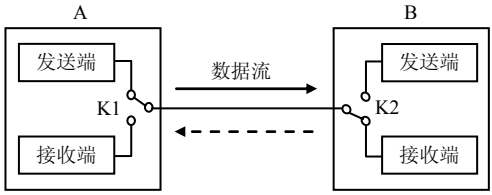



图 2-5　半双工通信

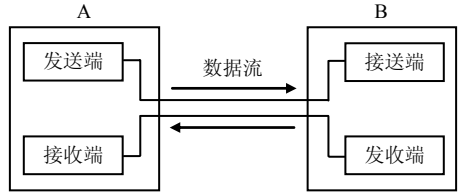



图 2-6　全双工通信

### 3．同步通信和异步通信

在数据通信系统中，通信双方收发数据序列必须在时间上取得一致，这样才能保证接收的数据和发送的数据一致，这就是通信中的同步。在计算机网络中，串行通信广泛采用的通信方式有同步通信和异步通信两种；而并行通信则一般都是采用同步通信。

（1）异步通信

异步通信又称为群同步通信。在这种通信方式中，传输的信息被分成若干个“群”。所谓的“群”，一般是以字符为单位，在每个字符的前面加上起始位，在结束处加上终止位，从而组成一个字符序列。数据在传输的过程中，字符与字符之间的间隔时间是任意的，即字符间采用异步定时，但字符中的各个比特用固定的时钟频率传输。所以，在数据通信中，习惯上称为“异步通信”。

异步通信由于附加了起始位和终止位，增加了传输开销，所以传输效率有所下降。但如果出现错误，只需重发一个字符，且这种方式简单，实现容易，适用于低速率场合。

（2）同步通信

同步通信是指接收端收到的每一位数据都要和发送端准确地保持同步，中间无间断时间，实现这种同步的方法可分为外同步法和自同步法两种。

在外同步法中，接收端的同步信号事先由发送端传来，而不是自己产生，也不是从信号中提取出来的。即在发送数据之前，发送端先向接收端发出一串同步时钟脉冲，接收端按照这个时钟脉冲的频率和时序锁定接收频率，以便在接收数据的过程中始终与发送端保持同步。然后向发送端发送准备接收的确认信息，发送端接收到确认信息后，开始发送数据。

自同步法是指接收端能从接收到的数据信号波形中提取同步信号的方法。在传输代码信息时，也将时钟同步信号一起传输给对方。

与异步传输相比，同步传输的数据是整批的，比异步通信一次一个字符，具有较高的传输效率和速率。

## 2.1.4　数据通信中的主要技术指标

在数据通信中，衡量和评价一个系统的好坏，涉及系统的主要性能指标问题，其中有 4 个指标是非常重要的，即数据传输速率、信道容量（也称“数据传输带宽”）、时延和误码率。

### 1．数据传输速率

（1）比特率

数字信道传送数字信号的速率即单位时间内所传送的二进制位的个数称为比特率或数据传输速率。单位为比特每秒，表示为 bps 或 b/s。数据传输速率的计算公式为

$$S = (1/T)\log_2 N$$

其中：

$S$ 表示比特率；

$T$ 表示脉冲宽度；

$N$ 表示一个脉冲所表示的有效状态数，即调制电平数，通常为 2 的整数倍。

（2）波特率

波特率又称码元速率或调制速率，指单位时间内所传送的码元的个数，单位为 baud（波特），可用如下公式表示：

$$B = 1/T$$

其中：

$B$ 表示波特率

$T$ 表示信号周期。

例如，若一连续信号 $f$=1600Hz，则 $B = 1/T$ =1600（波特）

（3）比特率与波特率的关系

比特率与波特率都是衡量信息在传输线路上传输快慢的指标，但两者针对的对象有所不同。比特率针对的是二进制位数传输，波特率针对的是信号波形的传输。二者之间的关系如下：

$$S = B\log_2 N$$

2．数据传输带宽

“带宽”有以下两种不同的意义：

（1）带宽本来是指某个信号具有的频率宽度。例如，在传统的通信电话线路中传输的语音信号的标准带宽是 3.1kHz（从 300～3 400Hz，即语音的主要成分的频率范围）。这种意义的带宽的单位是赫兹。带宽有信道带宽和信号带宽的区别。

（2）在计算机网络中，当通信线路用来传送数字信号时，传送数字信号的速率即数据传输率就应当成为数字信道的最重要的指标，不过习惯上仍延续使用“带宽”作为“数据传输率”的同义语，我们应联系上下文正确区分“带宽”的含义。当带宽表示数字信号的发送速率时，带宽有时也称为“吞吐量”。

3．时延

时延就是信息从网络的一端传送到另一端所需的时间。时延由发送时延、传播时延、处理时延构成。

## 2.2 数据传输介质

### 2.2.1 传输介质的基本概念

数据传输介质是传送信息的载体，是通信网络中发送方与接收方之间的物理通路。因此，传输介质也称为传输媒体、传输媒介或传输线路。

1．传输介质的分类

通信介质分为有线介质和无线介质两大类。网络中常用的有线介质是双绞线、同轴电缆和光纤；无线介质是无线电波、微波和红外线等。

2．传输介质的特性

数据传输的质量除了与传送的数据信号及收发两端的设备特性有关外，还直接与通信线路本身的机械和电气特性有关。这些特性主要包括：① 物理特性：指传输介质的特征。② 传输特性：传输信号调制技术、信道容量及传输的频带范围。③ 覆盖地理范围：指的是在不用中继设备的情况下，无失真传输所能达到的最大距离。④ 抗干扰特性：指防止噪声对传输信息影响的能力。⑤ 价格：指线路安装、维护等费用的总和。

### 2.2.2 双绞线（Twisted Pair）

双绞线是由两条相互绝缘的导线按照一定的规格互相缠绕（一般以顺时针缠绕）在一起而制成的一种通用配线如图 2-7 所示，属于信息通信网络传输介质。双绞线过去主要是用来传输模拟信号的，但现在同样适用于数字信号的传输。双绞线是目前使用最广泛、价格最低廉的一种有线传输介质。

双绞线采用了一对互相绝缘的金属导线互相绞合的方式来抵御一部分外界电磁波干扰，

更主要的是降低自身信号的对外干扰。把两根绝缘的铜导线按一定密度互相绞在一起，可以降低信号干扰的程度，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。“双绞线”的名字也是由此而来。

图 2-7　双绞线

双绞线芯一般是铜质的，能提供良好的传导率。双绞线一般分为非屏蔽双绞线（UTP）和屏蔽双绞线（STP）两种。

### 1．非屏蔽双绞线

非屏蔽双绞线由 8 根铜缆组成，其中这 8 根线由绝缘体分开，并且将一对或多对双绞线线对放入一个绝缘套管中，如图 2-8 所示。

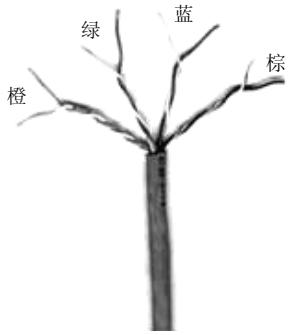



图 2-8　非屏蔽双绞线

非屏蔽双绞线非常适合于楼宇内部的结构化布线。具有尺寸小、质量小、易于弯曲、易安装和易维护等特点。使用标准 RJ-45 连接器，局域网大多数用户是使用双绞线连接而成的。

双绞线的种类有以下几种。

（1）一类线：主要用于语音传输（一类标准主要用于 20 世纪 80 年代初之前的电话线缆），不同于数据传输。

（2）二类线：传输频率为 1MHz，用于语音传输和最高传输速率为 4Mbps 的数据传输，常见于使用 4Mbps 规范令牌传递协议的旧的令牌网。

（3）三类线：指目前在 ANSI 和 EIA/TIA 568 标准中指定的电缆，该电缆的传输频率 16MHz，用于语音传输及最高传输速率为 10Mbps 的数据传输，主要用于 10Base-T。

（4）四类线：该类电缆的传输频率为 20MHz，用于语音传输和最高传输速率 16Mbps 的数据传输，主要用于基于令牌的局域网和 10Base-T/100Base-T。

（5）五类线：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，传输率为 100Mbps，用于语音传输和最高传输速率为 100Mbps 的数据传输，主要用于 100Base-T 和 1000Base-T 网络。这是最常用的以太网电缆。

（6）超五类线：超五类线具有衰减小、串扰少，并且具有更高的衰减与串扰的比值（ACR）和信噪比（Structural Return Loss）、更小的时延误差等，性能也得到很大提高等特点。超五类线主要用于千兆位以太网（1 000Mbps）。

（7）六类线：该类电缆的传输频率为 1～250MHz，六类布线系统在 200MHz 时综合衰减串扰比（PS-ACR）应该有较大的余量，它提供 2 倍于超五类的带宽。六类布线的传输性能远远高于超五类标准，最适用于传输速率高于 1Gbps 的应用。六类与超五类的一个重要的不同点在于：改善了在串扰以及回波损耗方面的性能，对于新一代全双工的高速网络应用而言，优良的回波损耗性能是极重要的。六类标准中取消了基本链路模型，布线标准采用星形的拓扑结构，要求布线的距离为：永久链路的长度不能超过 90m，信道长度不能超过 100m。

（8）七类线：带宽为 600MHz，可能用于今后的 10 吉比特以太网。目前，计算机网络所使用的主要是超五类线。

**2．屏蔽双绞线**

屏蔽双绞线是在一对或多对双绞线线对的外面加上一个用金属丝编织成的屏蔽层，然后再放入一个绝缘套管，如图 2-9 所示。

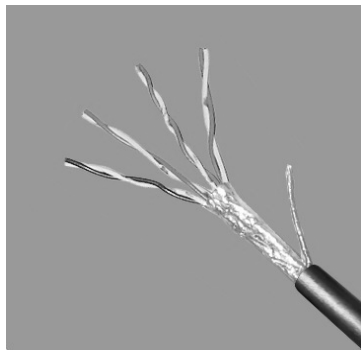


图 2-9　屏蔽双绞线

屏蔽双绞线是屏蔽技术和双绞线技术相结合的产物，具有较高的传输质量。屏蔽双绞线在线径上要明显粗过非屏蔽双绞线，而且由于它具有较好的屏蔽性能，所以也具有较好的电气性能。但由于屏蔽双绞线的价格较非屏蔽双绞线贵，且非屏蔽双绞线的性能对于普通的企业局域网来说影响不大，甚至说很难察觉，所以在企业局域网组建中所采用的通常是非屏蔽双绞线。不过七类双绞线除外，因为它要实现全双工 10Gbps 速率传输，所以只能采用屏蔽双绞线，而没有非屏蔽的七类双绞线。六类双绞线通常也建议采用屏蔽双绞线。

随着网络技术的发展和应用需求的提高，双绞线这种传输介质标准也得到了一步步的发展与提高。从最初的一、二类线，发展到今天最高的七类线，而且据悉这一介质标准还有继续发展的空间。在这些不同的标准中，它们的传输带宽和速率也相应得到了提高，七类线已达到 600MHz，甚至 1.2GHz 的带宽和 10Gbps 的传输速率，支持千兆位以太网的传输。

## 2.2.3　同轴电缆

同轴电缆是网络应用中十分广泛的传输介质之一，它以硬铜线为芯，外包一层用密织的网状导体环绕的绝缘材料，网外又覆盖一层保护性材料。同轴电缆由 4 层按“同轴”形式构成，如图 2-10 所示。

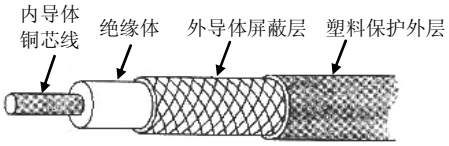



图 2-10　同轴电缆

同轴电缆比屏蔽双绞线或非屏蔽双绞线传输的距离远。因此，在没有中继器对信号放大的情况下，同轴电缆可以连接的局域网范围比双绞线大。但由于其曲折困难、质量大的缺点不适合用于楼宇内部的结构化布线。

同轴电缆有多种规格和型号。按应用环境可分为基带同轴电缆和宽带同轴电缆。基带同轴电缆一般只用来传输数据，不使用 Modem，因此，较经济，适合于距离较短、速度要求较低的局域网。基带同轴电缆的特性阻抗为 50Ω，有 RG-8 粗缆和 RG-58 细缆两种型号；宽带同轴电缆传输率高、传输距离远，但成本高。它不仅可以传输数据，还可以传输图像和声音信号等。宽带同轴电缆的特性阻抗为 75Ω，型号有 RG-59 等。

双绞线和光纤作为两大主流的有线传输介质被广泛使用，在目前的布线标准中已不再推荐使用同轴电缆。

### 2.2.4　光纤

光导纤维简称为光纤，是一种传输速率高达几百兆比特每秒、误码率极低的传输介质，也是网络传输介质中带宽最宽、传输速率最高、性能最好、应用前途最广泛的一种。光纤的材料可以是玻璃和塑料，其中使用超高纯度石英玻璃制作的光纤可以达到最低的传输损耗。

从横截面观察，每根光纤都被反射包层和外部保护层所包围。光纤的导光部分由光纤芯和包层构成。中心的光纤芯使用超高纯度的石英玻璃或塑料构成，其折射率很高。光纤芯外的包层由折射率较低的玻璃或塑料层组成，这样在光纤中传输的光将在光纤芯与包层的交界处形成全反射。光纤利用全反射将光线限制在光导玻璃中，即使在弯曲的情况下，光也能传输很远的距离。最外层的外部保护层是由塑料和其附属材料制成的，用于防止潮气、擦伤、压伤或外界的其他损害，如图 2-11 所示。

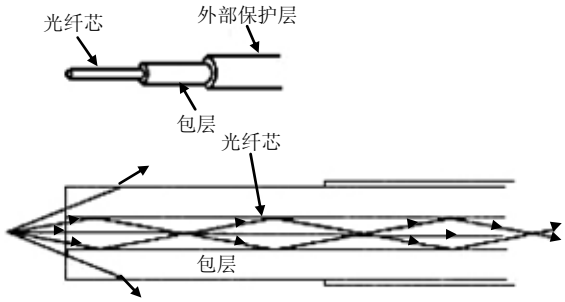



图 2-11　光纤及光纤原理结构图

光纤可分为单模光纤和多模光纤。多模光纤允许许多条不同角度入射的光线在一条光纤中传输，即有多条光路，传输衰减比较大，在无中继条件下，传播距离较短。但其耦合损失

较小，易于连接、价格低廉。故常用于中、短距离的数据传输网络和局域网中。单模光纤中光纤直径与光波波长相等，只允许一条光线在一条光纤中直线传输，即只有一条光路，在无中继条件下，传播距离较远。但这种光纤难以与光源耦合、连接困难、价格也较贵。故主要用于长距离主干线的传输。这两种光纤在局域网中都有其应用，单模光纤的传输质量比多模光纤的传输质量好，因此，单模光纤可以用于传输远距离的、覆盖范围较广的网络中。

光纤与 UTP、STP 和同轴电缆相比，光纤的传输速率更高。由于在光纤中传输的是光而不是电磁波，所以既不受电磁波的干扰，也不受无线电的干扰，更不会成为雷电的接入点。但是，尽管光纤细如发丝，其价格却十分昂贵，安装也比较困难。并且在光连接器的接口处必须十分光滑，不能有划痕。

### 2.2.5 无线介质

使用无线介质，是指在两个通信设备之间不使用任何物理的连接器，即无须铺设网络传输线。常用的无线介质包括无线电、微波、卫星、红外线和移动通信等。在计算机网络领域内，无线介质主要是微波，也有使用红外线进行通信的。微波通信常用的有地面微波通信和卫星通信两种。

#### 1．地面微波通信

由于微波在空间是直线传播的，而地球表面是个曲面，因此其传输距离受到限制，一般只有 50km 左右。若采用架高的天线塔，则传输距离可增大。它的优点是频带宽、信道容量大、初建费用小，既可传输模拟信号，又可传输数字信号；其缺点是方向性强（必须直线传播）、保密性差。

#### 2．卫星通信

卫星通信实际上是使用人造地球卫星作为中继器构成的微波通信。通信卫星通常被定位在几万公里的高空，卫星作为中继器可使信息的传输距离很远。卫星通信已被广泛用于远程计算机网络中，如图 2-12 所示。它的优点是容量大、可靠性高、通信成本与两站点之间的距离无关，传输距离远、覆盖面广、具有广播特征；缺点是一次性投资大、受自然环境影响大和传输延迟时间长。

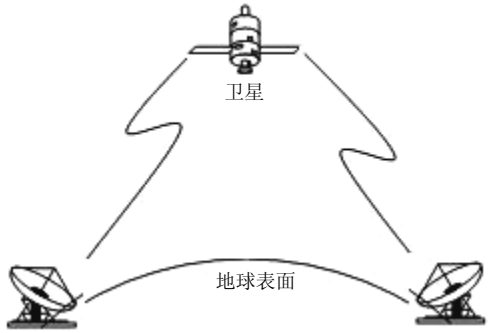



图 2-12　卫星通信

无线通信除了微波及卫星通信外，还有红外线、激光等介质。红外线和激光通信的收发

设备必须处于视线范围内，均有很强的方向性，因此，防窃取能力强，但由于它们的频率太高，对环境因素较敏感，因而只能在室内和近距离使用。

## 2.3　数据编码与传输技术

数据通信是通过信道在信源与信宿之间进行的信息交流。信息在信源或信宿处，既可以是模拟数据，也可以是数字数据；同样，在信道中既可以传输模拟信号，也可以传输数字信号。

通过模拟信道进行的数据通信称为模拟数据通信；通过数字信道进行的数据通信称为数字数据通信。

### 2.3.1　模拟数据通信和数字数据通信

#### 1．模拟数据通信

模拟数据（Analog Data）是由传感器采集得到的连续变化的值，如温度、压力，以及目前在电话、无线电和电视广播中的声音和图像。

模拟数据通信是利用模拟信道传输数据，有以下两种典型形式：

（1）模拟信道传输模拟数据。例如，声音在普通电话系统中的传输。

（2）模拟信道传输数字数据。例如，通过电话系统实现两台计算机（数字设备）之间的通信。由于电话系统只能传输模拟信号，所以需通过调制解调器（Modem）进行数字信号与模拟信号的转换。

#### 2．数字数据通信

数字数据（Digital Data）则是模拟数据经量化后得到的离散的值，如在计算机中用二进制代码表示的字符、图形、音频与视频数据。数字数据通信是利用数字信道传输数据，有以下两种典型形式：

（1）数字信道传输模拟数据。需要对模拟数据进行数字信号编码，这一工作可通过编码解码器（CODEC）完成。

（2）数字信道传输数字数据。例如，将两个计算机通过接口直接相连。

#### 3．模拟数据通信与数字数据通信的比较

模拟数据长距离传输时，需用放大器增加信号中的能量。虽克服了衰减，但增加了噪声。数字数据通信长距离传输时，需用中继器增加信号中的能量。这样既克服了衰减，又不增加噪声，可以做到信号的完全复原。因此，数字数据通信有着更为广阔的发展前景。

### 2.3.2　数据编码与调制

#### 1．数字数据的数字信号编码

利用数字通信信道直接传输数字数据，在传输之前需要进行数字信号编码。数字信号的

编码方式主要有 4 种：不归零编码、归零码、曼彻斯特编码和差分曼彻斯特编码。

（1）不归零编码 NRZ（Non-Return Zero）

在 NRZ 编码中，二进制数字 0、1 分别用两种电平来表示，它是一种全宽码，即信号波形在一个码元全部时间内发出或不发出电流，每一位码元占用全部码元宽度。不归零码又可分为单极性不归零码和双极性不归零码。

① 单极性不归零码

单极性不归零码是以无电压表示“0”，用恒定的正电压表示“1”。例如，二进制数 011101001 的单极性不归零码脉冲如图 2-13 所示。

② 双极性不归零码

双极性不归零码是以负电压表示“0”，用恒定的正电压表示“1”。例如，二进制数 011101001 的双极性不归零码脉冲如图 2-14 所示。

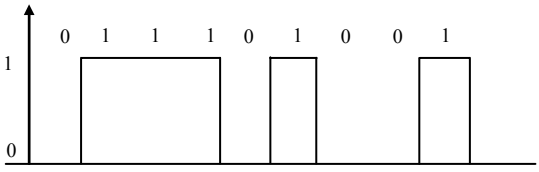



图 2-13　二进制数 011101001 的单极性不归零码脉冲

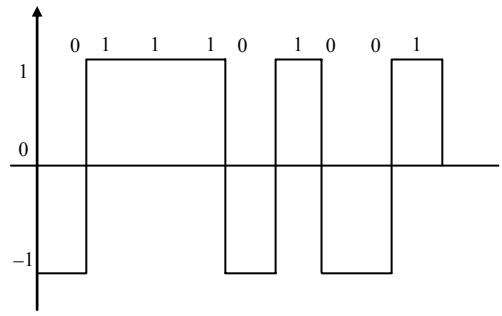
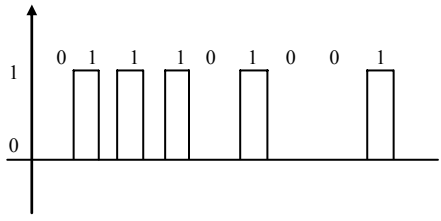


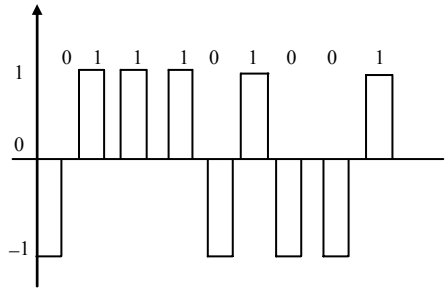

图 2-14　二进制数 011101001 的双极性不归零码脉冲

（2）归零码

归零码就是一个码元的信号波形不占用码元的全部时间，即在一个码元时间内发出电流的时间短于一个码元的时间宽度，发出的是窄脉冲。所以不管码元发出还是不发出电流，码元波形都归零。因此这种编码称为归零码。二进制数 011101001 的单极性归零码脉冲和双极性归零码脉冲如图 2-15（a）、（b）所示。




（a）单极性归零码脉冲




（b）双极性归零码脉冲

图 2-15　二进制数 011101001 的归零码脉冲

（3）曼彻斯特编码

在曼彻斯特编码中，首先将一个码元时间一分为二，如果在前半个码元时间里，电压为高电压，在码元的中间发生电压跳变，即从高电平跳到低电平，此时表示“0”；反之，如果在一个码元的中间从低电平跳到高电平，则表示“1”。二进制数 01001011 的曼彻斯特编码如

图 2-16 所示。

（4）差分曼彻斯特编码

差分曼彻斯特编码也是首先将一个码元时间一分为二，如果在一个码元开始处有跳变（跳变的方向根据前一码元的后半周期而定），则表示“0”，如果在一个码元开始处无跳变，则表示“1”。但任何波形都在码元的中间位置进行跳变。二进制数 01001011 的差分曼彻斯特编码如图 2-16 所示。

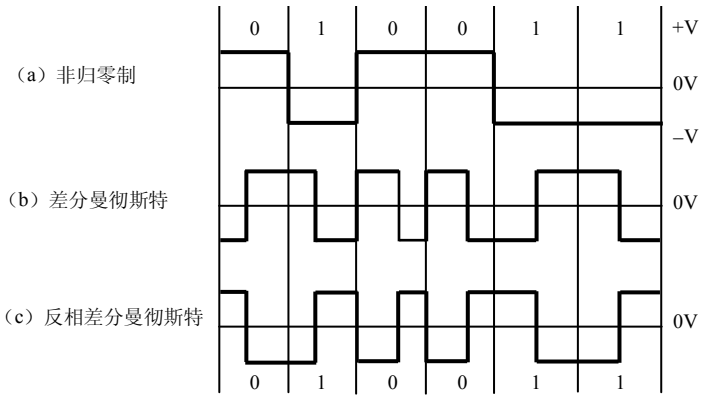



图 2-16　二进制数 011101001 的曼彻斯特编码和差分曼彻斯特编码

### 2．数字数据的模拟信号调制

典型的模拟通信信道是电话通信信道，它是为传输语音信号设计的，用于传输音频 300～3 400Hz 的模拟信号，不能直接传输数字信号。为了利用电话交换网的模拟语音信道实现计算机数字信号的传输，必须将数字信号转化为模拟信号。

要在模拟信道上传输数字数据，首先数字信号要对相应的模拟信号进行调制，由于模拟信号是具有一定频率的连续的载波波形，所以可以用模拟信号作为载波运载要传送的数字数据。

载波信号可以表示为正弦波形式：$f(t)=A\sin(\omega t+\varphi)$，其中幅度为 $A$、频率为 $\omega$ 和相位为 $\varphi$ 的变化均影响信号波形。因此，通过改变这 3 个参数可实现对模拟信号的编码。相应的调制方式分别称为幅度调制 ASK、频率调制 FSK 和相位调制 PSK。结合 ASK、FSK 和 PSK 可以实现高速调制，常见的组合是 PSK 和 ASK 的结合。

（1）幅度调制 ASK

幅度调制也称为幅移键控，简称调幅。在幅度调制中，载波信号的频率 $\omega$ 和相位 $\varphi$ 是常量，幅度 $A$ 是变量，即用载波的两种不同的振幅来表示二进制值的两种状态。用振幅恒定的载波的存在表示“1”，用载波的不存在表示“0”，如图 2-17 所示。

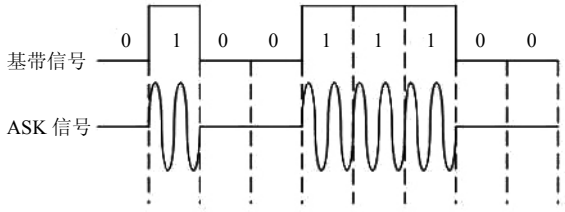



图 2-17　幅度调制

幅度调制是一种效率相当低的调制技术。

（2）频率调制 FSK

频率调制称频移键控，是把振幅 $A$ 和相位 $\phi$ 作为常量，而用载波频率附近的两个不同频率来表示两个二进制值。以频率较低的信号状态代表“0”，以频率较高的信号状态代表“1”。如图 2-18 所示。

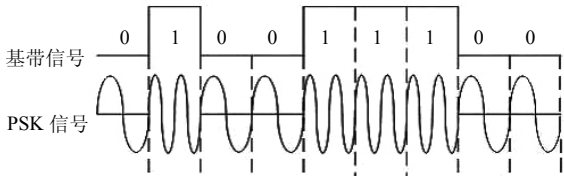



图 2-18　频率调制

（3）相位调制 PSK

相位调制也称为相移键控，是把振幅和频率定义为常量，而用相位的变化来表示二进制值的变化。相移键控又可分为绝对相移键控 APSK 和相对相移键控 DPSK。

① 绝对相移键控

所谓绝对相移键控就是利用载波的不同相位直接表示数字“0”和数字“1”。用公式可表示为

$$U(t) = A\sin(\omega t + \pi) \quad \text{数字“0”}$$

$$U(t) = A\sin(\omega t + 0) \quad \text{数字“1”}$$

② 相对相移键控

相对相移键控是用载波在两位数字信号的交接处产生的相位偏移来表示载波所表示的数字信号。最简单的相对调相方法是：与前一个信号同相表示数字“0”，相位偏移 180 度表示“1”，这种方法具有较好的抗干扰性。

### 3．模拟数据的数字信号编码

当利用数字通信介质传送模拟信号时就要对模拟数据进行数字信号编码。最常用的方法是脉冲编码调制 PCM（Pulse Code Modulation），它常用于对声音信号进行编码。PCM 处理信号分为 3 个步骤：采样、量化和编码。

采样：指每隔一定的时间间隔，采集模拟信号的瞬时电平值作为样本表示模拟数据在某一区间随时间变化的值。采样频率以采样定理为依据，如果以等于或高于最高有效信号频率两倍的速率定时对信号进行采样，这些采样值就包含了原始信号的全部信息。

量化：指将采样样本幅度按量化级决定取值的过程，经过量化后的样本幅度为离散的量化级值，将采样所得样本的幅值与量化级的幅值比较，取整定级。

编码：使用相应位数的二进制代码表示量化后的采样样本的量级。若量化的范围在 0～127，则每个采样要用 7 位二进制数（$2^7$=128）来表示；若量化的范围在 0～255，则每个采样需要用 8 位二进制数（$2^8$=256）来表示。

PCM 处理信号的过程如图 2-19 所示。

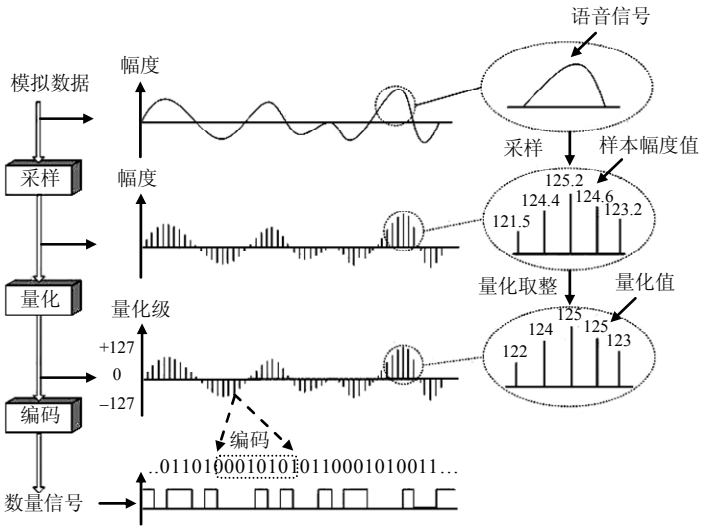



图 2-19　PCM 处理信号的过程

当 PCM 编码用于数字化带宽为 4kHz 的语音系统时，如果将声音分为 128 个量化级，每个量化级需用 7 位二进制编码表示，采样频率为 8 000 样本/秒时，数据传输率为 7 × 8 000=56Kbps。

此外，PCM 还可以用于计算机中的图形、图像数字化以及传输处理等。采用 PCM 二进制编码的缺点是使用的二进制位数较多，编码效率低。

## 2.3.3　基带传输与频带传输

### 1．基带传输

基带传输又叫称为数字传输，是指由计算机或终端等数字设备产生的、未经调制的数字数据相对应的电脉冲信号，它所占据的频率范围从直流和低频开始，因而这种电脉冲信号被称为基带信号。基带信号所占有的频率范围称为基本频带，简称基带。在信道中直接传输这种基带信号的传输方式就是基带传输。基带信号的能量在传输过程中很容易衰减，在没有信号放大的情况下一般不大于 2.5km，因此基带传输多用于短距离的数据传输。

### 2．频带传输

远距离通信信道多为模拟信道，如传统的电话（电话信道）只适用于传输音频范围（300～3 400Hz）的模拟信号，不适用于直接传输频带很宽、但能量集中在低频段的数字基带信号。

频带传输就是先将基带信号变换（调制）成便于在模拟信道中传输的、具有较高频率范围的模拟信号（称为频带信号），再将这种频带信号在模拟信道中传输。由于频带信号是模拟信号，频带传输实际上就是模拟传输。

计算机网络的远距离通信通常采用的是频带传输。基带信号与频带信号的转换是由调制解调技术完成的。

# 2.4 多路复用技术

在通信系统中，如果一个信道只传送一路信号是非常浪费的。复用就是指在同一通信介质上同时传输多个不同的信号。采用信道多路复用技术，可以将多路信号组合在一条物理信道上进行传输，在接收端再用专门的设备将各路信号分离开来，极大地提高了通信线路的利用率，如图 2-20 所示。实行多路复用的前提是信道的实际传输能力超过单个信号所要求的能力，即对信道的带宽和传输能力有较高的要求。

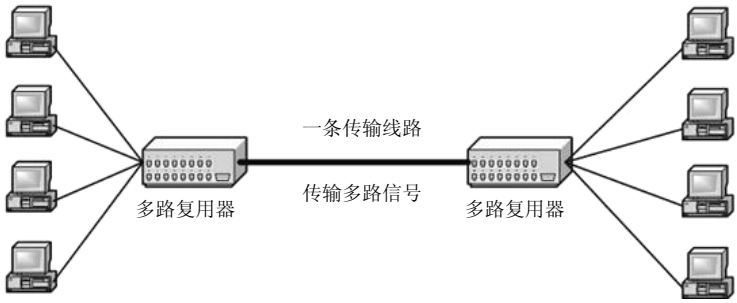



图 2-20 复用的概念

常用的多路复用技术有频分多路复用、时分多路复用和波分多路复用三种。

### 1．频分多路复用

频分多路复用 FDM（Frequency Division Multiplexing）是指载波带宽被划分为多种不同频带的子信道，每个子信道可以并行传送一路信号的一种技术。FDM 常用于模拟传输的宽带网络中。

在频分多路复用系统中，信道的可用频带被分成若干个互不交叠的频段，每路信号用其中一个频段传输，因而可以用滤波器将它们分别过滤出来，然后分别解调接收。

频分多路复用的优点是：信道复用率高，分路方便，因此频分多路复用是目前模拟通信中常采用的一种复用方式，特别是在有线和微波通信系统中应用十分广泛。频分多路复用的实现条件是信道所能提供的带宽要比传送一路信号所需的带宽宽得多。

频分多路复用也存在一些问题，主要表现在各路信号之间的相互干扰，即串扰。引起串扰的主要原因是滤波器特性不够理想和信道的非线性特性，信道的非线性失真改变了它的实际频带特性，易造成串音和互调噪声干扰。因而在频分多路复用系统中对系统线性的要求很高。合理选择载波频率，并在各路已调信号频谱之间留有一定的空闲频带，以作为保护频带，也是减小串扰的有效措施。

### 2．时分多路复用

时分多路复用 TDM（Time Division Multiplexing）是将一条物理信道的传输时间分成若干个时间片，按一定的次序轮流给各个信号源使用。因此，使用 TDM 的前提是：物理信道能达到的数据传输速率超过各路信号源所需的数据传输速率。

确定每个信道何时使用线路的时分多路复用方式称为同步时分多路复用（STDM）；反之

则称为异步时分多路复用（ATDM）。时分多路复用常用于基带网络中。

（1）同步时分多路复用

同步时分多路复用是指分配给每个终端数据源的时间片是固定的，不管该终端是否有数据发送，属于该终端的时间片都不能被其他终端占用。在接收端，根据时间片序号可判断出是哪一路信号。同步时分多路复用不能充分利用信道容量，从而造成资源的浪费。

（2）异步时分多路复用

异步时分多路复用又称为统计时分多路复用，允许动态地分配时间片，如果某个终端不发送信息，则其他终端可以占用该时间片。从统计角度来讲，所有的终端同时要求分配信道的可能性是很小的，因此异步时分多路复用可以为更多的用户服务。

频分多路复用主要用于模拟信道的复用，时分多路复用主要用于数字信号的复用。

#### 3．波分多路复用

波分多路复用 WDM（Wavelength Division Multiplexing）是指在一根光纤上使用不同的波长同时传送多路光波信号的一种技术。WDM 应用于光纤信道。

WDM 和 FDM 基本上都基于相同原理，所不同的是 WDM 应用于光纤信道上的光波传输过程。波分多路复用的工作原理如图 2-21 所示。要传输的光波的波长（频率）是不同的，它们通过合波器（通常是棱镜或光栅）后，就可使用一条共享的光纤传输，到达目的地节点后，再经过分波器（棱镜或光栅）分成多束光波。因此，波分多路复用并不是什么新的概念，只要每个信道由各自固有的频率范围而且信道间频率范围不相重叠，它们就能以多路复用的方式通过共享光纤进行远距离传输。

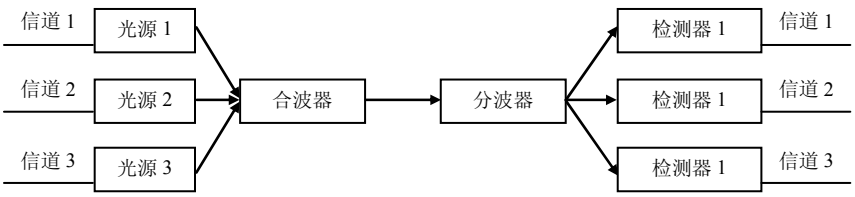



图 2-21　波分多路复用的工作原理

## 2.5　数据交换技术

### 2.5.1　数据交换的基本概念

各种数据经过编码后都可以在通信线路上进行传输，最简单的形式是用传输介质将两个端点直接连接起来进行数据传输。但这种方式是不现实的。这就需要设置交换节点，通过交换节点的某种连接方式来实现从任意一端到另一端之间数据通路的连续的技术，称为交换技术，或称为交换方式。

在数据通信中，数据交换方式主要包括：电路交换方式和存储转发交换方式。其中存储转发交换又分为报文交换和分组交换。

### 2.5.2 电路交换

电路交换（Circuit Switching）又称为线路交换，是一种面向连接的服务。两台计算机通过通信子网进行数据电路交换之前，首先要在通信子网中建立一个实际的物理线路连接。最普通的电路交换例子是电话系统。电路交换是根据交换机结构原理实现数据交换的。其主要任务是把要求通信的输入端与被呼叫的输出端接通，即由交换机负责在两者之间建立起一条物理通路。在完成接续任务之后，双方通信的内容和格式等均不受交换机的制约。电路交换方式的主要特点就是要求在通信的双方之间建立一条实际的物理通路，并且在整个通信过程中，这条通路被独占。

#### 1．电路交换的过程

电路交换的过程可划分为电路建立、数据传输和电路拆除 3 个过程。

（1）电路建立

如同打电话一样，先要通过拨号在通话双方间建立起一条通路一样，数据通信的电路交换方式在传输数据之前，首先由一端发起呼叫，另一端进行回应，交换网建立连接，直到两端节点间建立起一条转换式数据通路，然后才开始进行数据传输。建立时要求通信双方都要处于可用状态，并且两者之间的线路要空闲。其信道的形成不是唯一的，如果二者之间的一条线路忙，则可选择其他的线路通过。

（2）数据传输

电路连接建立以后，数据就可以从源节点发送到中间节点，再由中间节点交换到终端节点。当然终端节点也可以经中间节点向源节点发送数据。这种数据传输有最短的传播延迟，并且没有阻塞的问题，除非有意外的线路或节点故障而使电路中断。但要求在整个数据传输过程中，建立的电路必须始终保持连接状态，通信双方的信息传输延迟仅取决于电磁信号沿媒体传输的延迟。

（3）电路拆除

数据传输完毕后，执行释放电路的动作。该动作可以由任意节点发出拆除请求，然后进行拆除，即把线路的控制权释放。被拆除的信道空闲后，就可被其他通信使用。

#### 2．电路交换的特点与优缺点

独占性：在建立电路之后、释放线路之前，即使节点之间无任何数据可以传输，整个线路仍不允许其他节点共享。就和打电话一样，我们讲话之前总要拨完号之后把这个连接建立，不管你讲不讲话，只要不挂机，这个连接是专为你所用的，如果没有可用的连接，用户将听到忙音。因此线路的利用率较低，并且容易引起接续时的拥塞。

实时性：一旦电路建立，通信双方的所有资源（包括线路资源）均用于本次通信，除了少量的传输延迟之外，不再有其他延迟，具有较好地实时性。电路交换设备简单，无须提供任何缓存装置。用户数据透明传输，要求收发双方自动进行速率匹配。

电路交换方式的优点是数据传输可靠、迅速，数据不会丢失，且保持原来的序列。缺点是在某些情况下，电路空闲时的信道容量被浪费；另外，如数据传输阶段的持续时间不长，电路建立和拆除所用的时间就得不偿失。因此，它适用于远程批处理信息传输或系统间实时性要求高的大量数据传输的情况。这种通信方式的计费方法一般按照预订的带宽、距离和时间来计算。

### 2.5.3　报文交换

报文交换属于存储转发交换。报文交换的数据传输单位是报文。所谓报文就是包括结点所要发送的数据及源节点地址、目的节点地址和其他控制信息在内的数据块。报文可随机发送，且长度不受限制。报文交换不需要在通信双方之间建立专用通路，而采用“存储转发”的方式。即当一方要发送报文时，先将包括目的节点地址在内的控制信息加到所要传输的数据上，形成报文，并发送到与其相连的某一节点上。节点在收到报文后，先检查报文有无错误，将报文暂存在本节点上，然后根据报文的目的节点地址及路由信息将报文转发到下一结点，就这样一直转发出去，直到报文到达目的节点为止。

与电路交换相比，报文交换具有下列优点：

（1）在传送报文的源节点与目的节点之间不需要建立一条专用通路。也就没有建立线路和拆除线路所需的时间。

（2）线路的利用率高。节点间可根据中间节点的状态选择不同的传输速率，能高效地传输数据。

（3）要求节点具有足够的报文数据存放能力。一般节点由微机或小型机担当。

（4）数据传输的可靠性高，每个节点在存储转发中都要对报文进行差错控制，即检错、纠错。

（5）报文交换系统可把一份报文同时向多个目的地发送。

报文交换的主要缺点是：由于采用了对报文的存储转发，节点存储转发的时延较大，不适合交互式通信；由于每个节点都要把报文完整地接收、存储、检错、纠错、转发，产生了时延，并且对报文长度没有限制，报文可以很长，这样就有可能使报文长时间的占用两端节点之间的链路，不利于实时交互通信。

### 2.5.4　分组交换

随着计算机的广泛应用，对数据交换提出了更高的要求。例如，如何适应从很低到很高范围内的不同速率的交换；为了适合用户实时通信的要求，网络延迟要小；有高的传输准确性和多样化的数据交换业务。这些电路交换和报文交换显然是不能满足的。分组交换的出现较好地解决了上述问题。

分组交换（Packet Switching）也称为包交换，属于存储转发技术。它是把一个报文分成若干个较小的报文分组，每个分组的长度有一个上限。在发送方将报文分割成若干个分组，每个分组有一个编号，各个分组经网络节点存储转发到达目的节点后，目的结点再按分组报文编号重组报文。

分组交换的具体过程又可分为数据报方式和虚电路方式两种。

#### 1．数据报方式

在数据报方式中，每个分组的传送是被单独处理的，就像报文交换中的报文一样。每个分组被称为一个数据报，每个数据报自身带有足够的地址信息。一个节点收到一个数据报后，根据数据报中的地址信息和节点所存储的路由信息，选择一个合适的路径，将数据报原样地

发送到下一个节点，直到到达目的地。数据报方式的数据交换过程如图 2-22 所示。其具体过程可分为以下几步：

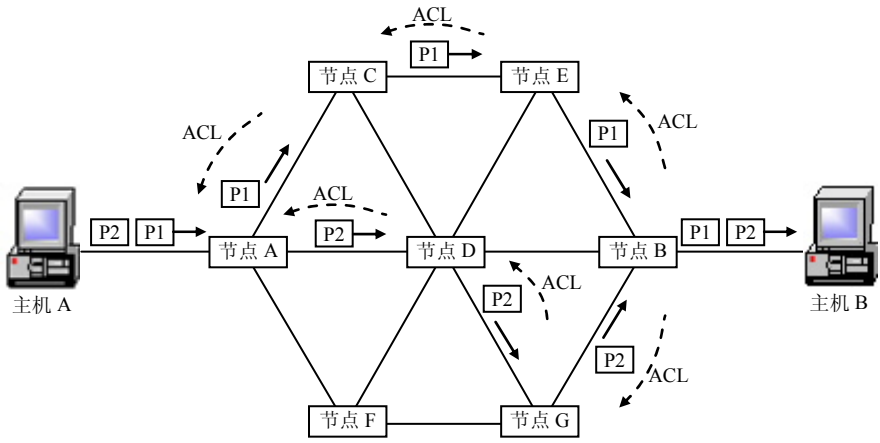



图 2-22　数据报方式的数据交换过程

（1）源主机将报文 M 分成多个分组 P1、P2 依次发送到与其直接连接的通信控制处理机（节点）A 上。

（2）节点 A 每接收一个分组都要进行差错检测，以保证源主机与节点 A 数据传输的正确性；节点 A 接收到分组 P1、P2 后，要为每个分组进入通信子网的下一个结点启动路由选择算法。由于网络的通信状态数是不断变化的，分组 P1 的下一个结点可能选择 C，而分组 P2 的下一个节点可能选择 D，因此同一报文的不同分组通过子网的路径可能是不相同的。

（3）节点 A 向节点 C 发送分组 P1 时，节点 C 要对 P1 传输的准确性进行检测。如果传输正确，节点 C 向节点 A 发送正确传输的确认信息；节点 A 收到节点 C 的确认信息后，确认 P1 已经正确传送，则废弃 P1 的副本。其他节点间的传输与交换过程与此类似。这样报文分组 P1 通过通信子网中的多个节点存储转发，最终到达目的节点 B。P2 及其他分组传输情况也类似。

（4）目的主机收到全部报文分组，按照报文分组的编号重新排列和组装，还原成原来的报文。数据报方式没有电路的呼叫建立过程，但要为每个数据报做路由选择。

### 2．虚电路方式

在虚电路（Virtual Circuit）方式中，为进行数据传递，网络的源节点和目的节点之间先要建立一条逻辑通路，如图 2-23 所示。假设源主机有一个或多个分组要发送到目的主机去，那么它首先要发送一个呼叫分组到 A 节点，请求建立一条到目的主机的连接。如此重复，经过节点 A→节点 F→节点 G→节点 B，节点 B 最终将呼叫请求分组传送到目的主机。如果目的主机接收这个连接，就发送一个呼叫接收分组沿原路线返回到源主机。这样一个从源主机到目的主机的逻辑连接就建立好了。至此，源主机就可以在已建立好的逻辑连接上或者说在虚电路上交换数据了。每个分组除了包含数据之外还得包含一个虚电路标识符。在预先建立好的路径上的每个节点都知道把这些分组信息引导到哪里去，不再需要路由选择判断。于是来自源主机的每一个分组都通过节点 A、F、G、B 到达目的主机，来自目的主机的每一个分组也都通过 B、G、F、A 节点到达源结点。通信结束后，由任何一方发出断开连接的请求，由另一端响应后，清除此虚电路。

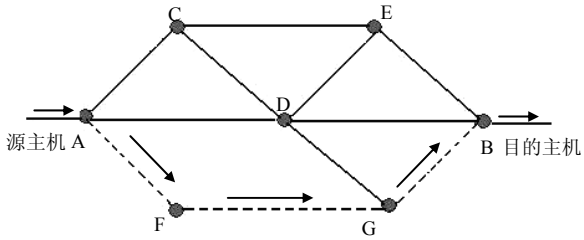



图 2-23　虚电路交换

无论何时，一个节点都能和任何节点建立多个虚电路，也能与多个节点建立虚电路。它之所以是“虚”的，就是因为这条电路不是专用的，虚电路在建立信道时，只会占用某条路径带宽的一部分，也就是说，此条路径的剩余带宽仍可以提供给其他用户使用。每条虚电路支持特定的两个端点之间的数据传输，两个端点之间也可以有多条虚电路为不同的进程服务，这些虚电路的实际路由可能相同也可能不同。虚电路方式具有如下特点：

（1）在每次发送数据之前，必须在发送方与接收方之间建立一条逻辑连接。这是因为不需要真正去建立一条物理链路。

（2）一次通信的所有分组都通过这条虚电路顺序传送，因此报文不必带目的地址、源地址等辅助信息，分组到达目的节点时不会丢失、重复和乱序等现象。

（3）分组通过虚电路上的每个节点时，节点只需做差错检测，不需要做路径选择。

（4）通信子网中的每个节点可以和任何节点建立多条虚电路连接。

## 2.6　差错控制技术

在解决了标识每一帧的起始和结束位置问题之后，还需要解决数据传输中的差错控制问题。就是如何确保所有的数据帧最终在递交给目标计算机上的网络层时，能保证数据的完整性，并且保持正确的顺序。因为在原始物理传输线路上存在着各种噪声和干扰，传输数据信号可能有差错。设计数据链路层的主要目的是将有差错的物理线路改进成无差错的数据链路，所采取的方法包括差错检测、差错控制和流量控制等。而在差错控制功能中，主要采取纠错码、反馈检测、自动重发等重传技术，下面分别予以介绍。

### 2.6.1　差错控制的基本概念

数据通信系统的基本任务是高效而无差错地传输数据。所谓“差错”，就是在通信接收端收到的数据与发送端实际发出的数据出现不一致的现象。差错的产生是不可避免的，数据从信源出发，经过通信信道进行传输，由于通信信道总是有一定的噪声存在，到达信宿时，接收信号将与噪声信号迭加。这样就可能导致差错的产生。通信信道中的噪声分为热噪声和冲击噪声，热噪声属于随机噪声，是通信信道上固有的、持续存在的，如线路本身电气特性随机产生的信号幅度、频率、相位的畸形和衰减，相邻线路之间的串扰等，这种噪声具有不固定性，由它引起的差错属于一种随机差错。冲击噪声是由外界某种原因突发产生的噪声，如雷电、电源开关的跳火、外界电磁场的变化等，由它引起的传输差错称为突发差错。

由于通信信道中的噪声的存在，不管信道质量多高，都要进行差错控制。差错控制是指数据通信过程中能发现或纠正错误，把差错限制在尽可能小的允许范围内的技术和方法。最常用的差错控制方法是差错控制编码，即数据信息在发送之前，先按照某种关系附加上一定的冗余位，构成一个码字后再进行发送。接收端在收到该码字后，检查信息位和附加的冗余位之间的关系，以检查传输过程中是否有差错发生。

## 2.6.2 差错控制的编码

差错控制编码分为检错码和纠错码。检错码是指能发现传输中的错误但不能自动纠正所发现的错误的编码，它需要通过反馈重新发来纠错；纠错码是指不仅能发现传输中的错误而且能自动纠正错误的编码。纠错码虽然能及时纠正传输错误，但实现复杂、造价高、费时，在一般通信场合不易采用。检错码需要通过重发机制达到纠错，但原理简单、实现容易、编码解码速度快，目前得到广泛采用。常见的检错码有奇偶校验码和循环冗余编码。

### 1．奇偶校验码

奇偶校验码是通过在数据后加上一个奇偶校验位，使得码字中“1”的个数为固定的奇数（奇校验）或偶数（偶校验）的编码方法，是一种检错码。如使用偶校验（“1”的个数恒为偶数）方式，则当“1”的个数为偶数时，在后面加一个“0”作为校验码，使其中的“1”个数仍为偶数；如果“1”的个数为奇数，则在后面加“1”作为校验码，仍保持其中的“1”个数为偶数。例如：

10110101 --> 101101011

10110001 --> 101100010

但奇偶校验码只可以用来检查单个错误，所以它检错能力差，一般只用于通信要求较低的环境。

### 2．循环冗余编码

循环冗余编码 CRC 简称循环码。CRC 码检错能力强，且容易实现，是目前最广泛的检错码编码方法之一。在计算机网络中，CRC 被广泛采用。

CRC 是一种检错码，其编码过程涉及多项式知识。也就是将二进制形式的码元看作是仅具有“0”或“1”两种取值的多项式的系数，$K$ 个码元看作是 $K$ 项多项式 $x^{k-1}+\cdots+x^0$ 表达式的系数。例如，比特串 100101011 可被解释成 $x^8+x^5+x^3+x+1$，而多项式 $x^8+x^6+x^4+x^2+x$ 对应的代码为 101010110。

CRC 的原理为：假设要传送的信息有 $k$ 位，则发送端会自动加上 $r$ 位的校验序列，然后再传送出去，$k+r$ 位数可以被某个事先设定好的数整除。当接收端收到数据后用原先那个设定好的数来除，若没有余数出现，则表示数据传送正确；否则，则表示数据传送有误。

CRC 码在发送端编码和接收端校验码时，都可以利用生成多项式 $G(x)$来得到。$K$ 位要发送的信息可对应（$k-1$）次多项式 $K(x)$，$r$ 位的冗余位则对应一个（$r-1$）次多项式 $R(x)$，有 $k$ 位信息位加 $r$ 位冗余位组成 $n=k+r$ 位码字对应于一个（$n-1$）次多项式 $T(x)=x^r\cdot K(x)+R(x)$。

由信息位产生冗余位的编码过程，就是已知 $K(x)$求 $R(x)$的过程。在 CRC 码中找到一个特

定的 r 次多项式 $G(x)$，然后利用 $x^r \cdot K(x)$ 去除以 $G(x)$，得到的余数就是 $R(x)$。CRC 码的方法如下：

（1）令 $r$ 为生成多项式 $G(x)$的阶，将 $r$ 个“0”附加在信息的低端，使其长度变为 k+r 位，即 $x^r \cdot K(x)$；

（2） $x^r \cdot K(x)$ 除以 $G(x)$，得到余数；

（3） $x^r \cdot K(x)$ 与余数对应位异或，得编码信息 $T(x) = x^r \cdot K(x) + R(x)$；

（4）接收端收到发来的编码信息后，用同一个生成多项式 $G(x)$去除编码信息，若余数为零，则表示接收到正确的编码信息，否则表示接收到的编码信息有误。

（5）将收到的正确编码信息 $T(x)$ 去掉尾部 $r$ 位，即得到数据信息 $K(x)$。

例如：要发送的信息多项式为 $K(x) = x^5 + x^4 + x + 1$，双方约定 $G(x) = x^4 + x^3 + 1$ 为生成多项式（$r$=4）。求 CRC 码的校验序列码，并验证收到的码字的正确性。

解：（1）信息码 110011 生成码为 11001。

（2） $x^r \cdot K(x)$ 的二进制位串为 1100110000（即在 $K(x)$ 的低位补 4 个“0”）。

（3）按模 2 除法计算 1100110000÷11001，得到余数 $R$=1001。模 2 除法的计算过程如图 2-24 所示。

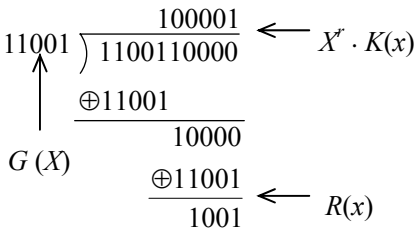



图 2-24　多项式除法

所以 $K(x)$ 的校验和为 1001；带校验和传送的信息为 1100110000+1001=1100111001。

接收端收到此码字后，用同一个生成多项式 $G(x)$去除编码信息，若余数为零，则表示接收到正确的编码信息，否则表示接收到的编码信息有误。

有时余数为零并不一定没有出现差错，可能在某种比特差错的组合下，也可能碰巧使得余数为零。但只要经过严格的挑选，并使用位数较多的除数 $G(x)$，出现检测不到差错的概率就可能很小了。现广泛使用的 $G(x)$有以下几种：

CRC12： $x^{12} + x^{11} + x^3 + x^2 + 1$

CRC16： $x^{16} + x^{15} + x^2 + 1$（IBM 公司）

CRC16： $x^{16} + x^{12} + x^5 + 1$（CCITT）

CRC32： $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

## 2.6.3　差错控制方法

如前所述，差错检测是通过差错控制编码来实现的。而差错纠正则通过差错控制方法来实现。常用的差错控制方法有反馈检测、自动请求重发和前向纠错。

### 1．反馈检测

反馈检测方法又称回送校验法。双方在进行数据传输时，接收方将接收到的数据重新发回发送方，由发送方检查是否与原始数据完全相符。如不相符，则发送方发送一个控制信息通知接收方删去出错的数据。并重新发送该数据；如相符，则发送下一个数据。

反馈检测方法的特点是：原理简单、实现容易、可靠性强，但开销大，信道利用率低。

### 2．自动请求重发

自动请求重发简称 ARQ（Automatic Repeat reQuest），是计算机网络中较常采用的差错控制方法。ARQ 的原理是发送方将要发送的数据附加上一定的冗余检错码一并发送，接收方则根据检错码对数据进行差错检测，如发现差错，则接收方返回请求重发的信息，发送方在收到请求重发的信息后，重新传送数据；如没有发现差错，则发送下一个数据，

为保证通信正常进行，还需引入计时器（防止整个数据帧或反馈信息丢失）和帧编号（以防止接收方多次收到同一帧并递交给网络层）。

其特点是使用检错码（常用的有奇偶校验码和 CRC 码等）、必须是双向信道、发送方需要设置缓冲器。

### 3．前向纠错

前向纠错简称 FEC（Forward Error Correction），其原理是发送方将要发送的数据附加上一定的冗余纠错码一并发送，接收方则根据纠错码对数据进行差错检测，如发现差错，由接收方进行纠正。

其特点是使用纠错码（纠错码编码效率低且设备复杂）、单向信道、发送方无须设置缓冲器。前向纠错方法在计算机网络中已不常使用。

## 练习 2

### 一、填空题

（1）数据通信的传输方式分为_____和_____，鼠标采用前者进行通信，打印机采用后者进行通信。

（2）在数据通信中，表征一个信道传输能力的指标是_____，衡量通信系统传输可靠性的指标是_____。

（3）用于计算机网络的传输介质有两类 _____和_____。

（4）对于双绞线，UTP 指_____，STP 指_____。

（5）目前主要信道复用方式有_____、_____和_____3 种，其中_____是用于光纤通信中。

（6）数字信号调制方式包括_____、_____和_____3 种。

（7）多路复用技术主要包括_____多路复用技术、_____多路复用技术和_____多路复用技术。

（8）实现分组交换的两种方法为_____和_____。

## 二、选择题

（1）下列说法正确的是（　　）。

A．模拟数据可以用模拟信号来表示

B．模拟数据也可以用数字信号来表示

C．数字数据可以用数字信号来表示

D．数字数据也可以用模拟信号来表示

（2）数据报和虚电路属于（　　）。

A．线路交换　　B．分组交换　　C．报文交换　　D．信元交换

（3）在下列传输介质中，不受电磁干扰或噪声影响的是（　　）。

A．双绞线　　B．通信卫星　　C．同轴电缆　　D．光纤

（4）使用调制解调器通过电话系统实现两个计算机之间的通信属于（　　）。

A．模拟信号传输模拟数据　　B．数字信号传输数字数据

C．数字信号传输模拟数据　　D．模拟信号传输数字数据

（5）下列说法正确的是（　　）。

A．串行通信方式比并行通信方式的效率高

B．并行通信方式比串行通信方式的效率高

C．并行通信方式和串行通信方式的效率一样

D．以上说法均不正确

（6）下列说法正确的是（　　）。

A．单工传输方式只有一个方向的数据传输

B．半双工可以有两个方向的数据同时传输

C．在七类双绞线中只有全双工传输方式

D．五类或超五类双绞线上只能进行半双工传输

（7）以太局域网是基带系统，它采用（　　）编码方式

A．归零　　B．4B/5B　　C．曼彻斯特　　D．不归零

（8）光纤分布数据接口 FDDI 标准中的数据编码采用的是（　　）。

A．4B/5B 编码　　B．曼彻斯特编码

C．双极归零编码　　D．双极不归零编码

（9）度量 Modem 进行数据传输时的最大速率的指标是（　　）。

A．数据传输率　　B．波特率　　C．位速率　　D．吞吐量

（10）下列数据交换方式中，线路利用率最高的是（　　）。

A．电路交换　　B．报文交换　　C．分组交换　　D．延迟交换

## 三、简答题

（1）简述数据通信系统模型的组成。

（2）数据分为模拟数据和数字数据，两者主要的区别有哪些？

（3）什么是带宽、信道容量、单工通信、半双工通信、双工通信、数据率、吞吐量和通信延迟？

（4）数据传输的基本方式、同步方式和复用方式各有哪些？并说明它们的工作原理和主

要特点。

（5）数据传输速率和信道容量之间的关系是什么？

（6）举例说明幅移键控、相移键控和频移键控 3 种调制方式原理。

（7）常用的传输介质有哪几种？各有什么特点？

（8）试比较电路交换、报文交换、虚电路分组交换和数据报分组交换的区别。

（9）在计算机网络中差错是如何产生的？通常采用何种方法检测和控制？

（10）已知要传送的数据为 1011011，生成多项式 $G(x)=x^4+x+1$，求其传送到接收端的 CRC 编码。

# 第 3 章

# 计算机网络体系结构

## 3.1 网络体系结构的基本概念

### 3.1.1 网络协议

计算机网络是一个涉及计算机技术、通信技术等多个领域的复杂系统。在网络中包含多种计算机系统，它们的硬件和软件系统各异。要使它们能协同工作以实现信息交换和资源共享，必须使它们采用统一的信息交换规则。在计算机网络中，把用于规定信息格式、信息内容以及如何发送和接收信息的一套规则（标准、约定）称为网络协议，或称通信协议。在计算机网络中要做到有条不紊地交换数据，就必须遵守一些事先约定好的网络协议。网络协议主要由下列 3 个要素组成：

（1）语法：语法规定通信双方彼此应如何操作，确定协议元素的格式，如用户数据和控制信息的格式和结构，即“如何讲”。

（2）语义：语义规定了通信双方要发出的控制信息、执行的动作和返回的应答等，即“讲什么”。

（3）定时：定时是对何时进行通信，有关事件实现顺序的详细说明，一般用状态图来描述，即“何时讲”。

例如，甲要打电话给乙，首先甲拨通乙的电话号码，对方电话振铃，乙拿起电话，然后甲乙开始通话，通话完毕后，双方挂断电话。 在这个过程中，甲乙双方都遵守了打电话的协议。

其中，电话号码就是“语法”的一个例子，一般电话号码由 5～8 位阿拉伯数字组成，如果是长途要加拨区号，国际长途还有国家代码等；两人之间的谈话选择使用什么语言也是语法。甲拨通乙的电话后，乙的电话振铃，振铃是一个信号，表示有电话打进，乙选择接电话，讲话；这一系列的动作包括了控制信号、响应动作、讲话内容等，就是“语义”的例子；“时序”的概念更好理解，因为甲拨了电话，乙的电话才会响，乙听到铃声后才会考虑要不要接，这一系列事件的因果关系十分明确，不可能没有人拨乙的电话而乙的电话会响，也不可能在电话铃没响的情况下，乙拿起电话却从话筒里传出甲的声音。

### 3.1.2 网络的分层结构

人类思维能力不是无限的，如果同时面临的因素太多，就不可能做出精确的思维。处理

复杂问题的一个有效方法，就是用抽象和层次的方式去构造和分析。在计算机网络中网络协议是不可缺少的。而一个功能完备的计算机网络需要制定一套复杂的协议集。对于这样的网络协议，就可以采用分层的组织方式。如图 3-1 所示，可将一个计算机网络抽象为若干层。其中，第 *N* 层是由分布在不同系统中的处于第 *N* 层的子系统构成，然后为每个子功能设计一个单独的协议，即每层对应一个协议。这样做使得每个协议的设计、分析、编码和测试变得简单易行。1980 年，H.Zimmerman 提出了网络层次划分原则，其要点如下：

（1）网络中各节点都有相同的层次。

（2）不同节点的同等层具有相同的功能。

（3）同一节点内相邻层之间通过接口通信。

（4）每一层使用下层提供的服务，并向其上层提供服务。

（5）不同节点的同等层按照协议实现对等层之间的通信。

通常不同的网络可以使用不同的网络协议，但只有使用了相同的协议，双方才易于通信，否则两个网络的连接之处还要进行必要的协议转换。

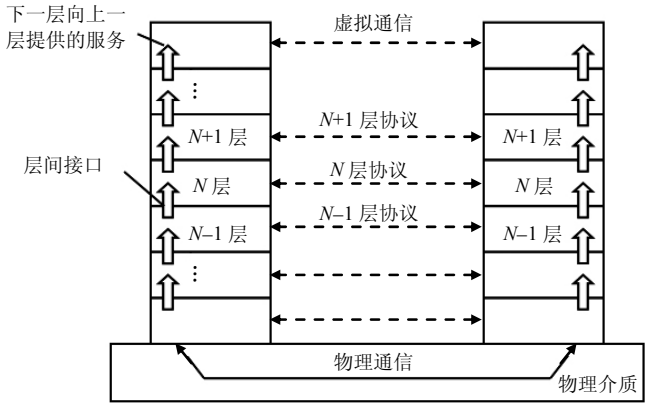



图 3-1　网络层次结构

计算机网络结构采用结构化层次模型，具有以下优点：

（1）把网络操作分成复杂性较低的单元，结构清晰，易于实现和维护。

（2）定义并提供了具有兼容性的标准接口。

（3）使设计人员能专心设计和开发所关心的功能模块。

（4）独立性强——上层只需了解下层通过层间接口提供什么服务—黑箱方法。

（5）适应性强——只要服务和接口不变，层内实现方法可任意改变。

（6）一个区域网络的变化不会影响另外一个区域的网络，因此每个区域的网络可单独升级或改造。

### 3.1.3　网络的体系结构

所谓网络体系就是为了完成主机之间的通信，把网络结构划分为有明确功能的层次，并规定了同层次虚通信的协议及相邻层之间的接口及服务。因此，网络的层次结构模型与各层协议和层间接口的集合统称为网络体系结构（Network Architecture）。

网络体系结构就是一种黏合剂，它使这些用不同媒介连接起来的不同设备和网络系统在不同的应用环境下实现互操作性，并满足各种业务的需求，它营造了一种“生存空间”，任何厂商的任何产品，以及任何技术只要遵守这个空间的行为规则，就能够在其中生存并发展。

#### 1．服务和接口

服务在计算机网络中是一个很重要的概念。在网络体系结构中，所谓服务就是网络中的各层向其相邻上层提供的一组操作，是相邻两层之间的界面。由于网络分层结构中的单向依赖关系，使得网络中相邻层之间的界面也是单向的。

在研究网络进行信息交换时，实体是系统中具有一定功能、能发送或接收信息的一种元素，它可以接收参数（输入），也可以产生效果（输出）。实体即可以指硬件的芯片，也可以指软件的进程，因为凡是具有一定功能的处理模块原则上都是实体。实体是构成系统的成分，在分层的体系结构中各系统的实体也分布在各层之中。每一层至少存在一个实体，在不同的主机上，同一层内的实体称为对等实体或称为对等进程。

#### 2．协议和服务的关系

首先，协议的实现保证了能够向上一层提供服务。本层的服务用户只能看见服务而无法看见下面的协议。下面的协议对上面服务的用户是透明的。

其次，协议是“水平的”，即协议是控制对等实体之间通信的规则。但服务是“垂直的”，即服务是由下层向上通过层间接口提供的。上层使用下层所提供的服务必须通过与下层交换一些命令，这些命令在 OSI 中称为服务原语。

## 3.2　OSI 参考模型

为了实现不同厂家生产的计算机系统之间及不同网络之间的数据通信，就必须遵循相同的网络体系结构模型，否则异种计算机就无法连接成网络，这种共同遵循的网络体系结构模型就是国际标准——开放系统互连参考模型，即 OSI/RM，所谓“开放”是指只要遵循 OSI 标准，一个系统就可以与位于世界上任何地方、遵循同一标准的其他任何系统进行通信。

### 3.2.1　OSI 参考模型简介

#### 1．OSI 参考模型的结构

OSI 发布的最著名的 OSI 标准是 ISO/IEC 7498 国际标准，又称为 X.200 建议，国际标准化组织为解决异种机互连而制定的开放式计算机网络层次结构模型。OSI 参考模型只是描述了一些概念，用来协调进程间通信标准的制定。将 OSI/RM 依据网络的整个功能划分成 7 个层次，以实现开放系统环境中的互连性（Interconnection），互操作性（Interoperation）和可移植性（Portability）。OSI 参考模型的推出，从理论上为网络的发展指明了方向。

OSI 将整个通信功能划分为 7 个层次。分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 3-2 所示。

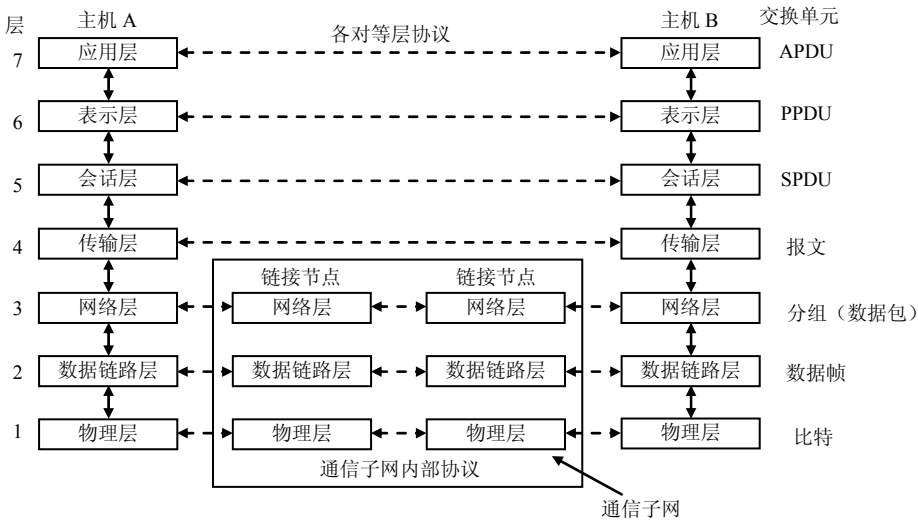



图 3-2　OSI 参考模型示意图

ISO/OSI 参考模型的特点：

（1）分层网络互连模型，分为两级结构（通信子网和资源子网）。

（2）只有物理层之间是直接连接的。

（3）对等层之间采用相同的对等协议。

（4）发送数据时，数据从高层到低层。

（5）接收数据时，数据从低层到高层。

### 2．OSI 参考模型的各层功能简介

（1）物理层

物理层的主要功能是为数据链路层提供一个物理连接，以保证在通信信道上“透明”地传输数据。传输介质可以是多种多样的，如双绞线、同轴电缆、光纤等。物理层协议的目的就是要屏蔽掉各种传输介质的差异性，以实现传输介质对计算机系统的独立性。该层的数据单元是比特流。

（2）数据链路层

数据链路层是为网络层提供服务的。它的主要功能是在物理层提供的服务基础上，在通信实体之间建立数据链路连接，无差错地传输数据帧。数据链路层协议的目的是把一条有可能出错的物理链路变成让网络实体看起来是一条不会出错的数据链路。该层的数据单元是帧。

（3）网络层

网络层是为传输层提供服务的。它的主要功能是为数据分组进行路由选择，并负责通信子网的流量控制、拥塞控制。该层的数据单元是数据包或分组。

（4）传输层

传输层的主要功能是为会话层提供一个可靠的端到端连接，以便使两个系统之间透明地传输报文。该层的数据单元是报文。

（5）会话层

会话层的主要功能是在传输层提供的端到端的连接的基础上，在两个应用进程之间建立

会话连接，并对“会话”进行管理，保证“会话”的可靠性。会话层及以上的数据单元都称为报文。

（6）表示层

表示层的主要功能是完成被传输数据的表示工作，如数据格式、数据转换和数据加密等语法变换服务。

（7）应用层

应用层作为参考模型的最高层，是用户与网络的接口。其功能与应用进程有关，如文件传输、收发电子邮件等。

### 3．OSI 参考模型中数据的传输过程

如图 3-3 所示，在 OSI 参考模型中数据的传输过程大致有以下几个过程。

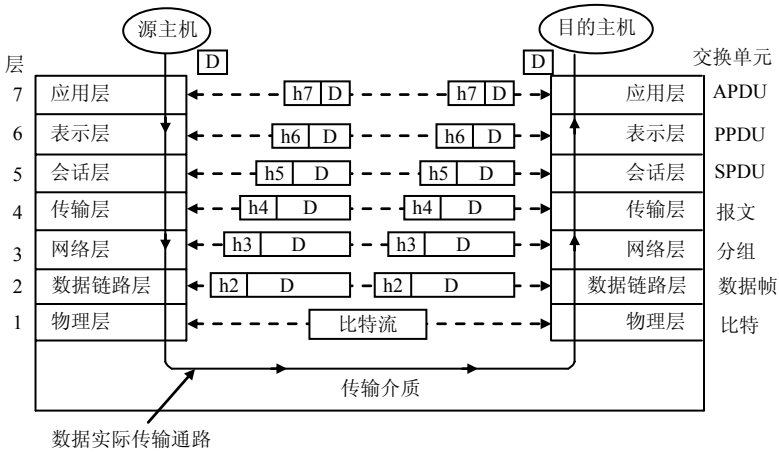



图 3-3　OSI 中数据的传输过程

（1）当源主机的应用进程的数据传送到应用层时，应用层加上本层的控制报头 AH，组成应用层的数据单元，然后送到表示层。

（2）表示层收到数据后，加上本层的控制报头 PH，组成表示层的数据单元，送到会话层。

（3）会话层收到数据后，同样加上本层的控制报头 SH，组成会话层的数据单元，送到传输层。

（4）传输层收到这个数据后，加上本层的控制报头 TH，组成传输层数据单元，送到网络层。

（5）传输层的报文送到网络层时，由于网络层的数据单元的长度的限制，传输层的报文将被分割成多个较短的数据段，加上网络层的控制报头 NH，构成网络层的数据单元，即分组。

（6）当网络层的分组到达数据链路层后，在分组的前后加上数据链路层的控制报头 DH，就构成了数据链路层的数据单元，即帧。

（7）数据链路层的帧到达物理层后，物理层将以比特流的方式，通过传输介质将其传输出去。

（8）当比特流到达目的主机时，再从物理层依次往上传输，每层去掉本层的控制报头，将数据上交到上一层，最终到达目的主机的应用进程。

对于网络中进行通信的主机进程来讲，OSI 环境中数据的传输过程是透明的，数据就像是直接送到目的地，这就是开放系统在网络通信过程中最主要的特点。

## 3.2.2 物理层

### 1．物理层概述

物理层是 OSI 参考模型中的最低层，也是最重要、最基础的一层。物理层即不是指连接计算机的具体物理设备，也不是指负责信号传输的具体物理介质，而是指在连接开放系统的物理介质上为上一层提供传输比特流的一种物理连接，它是建立在通信介质基础上的、实现设备之间联系的物理接口。即规定了为建立、维护和拆除物理链路（通信节点之间的物理路径）所需的机械、电气、功能和规程特性。其作用是确保比特流在物理信道上传输。

### 2．物理层的协议描述

物理层接口协议实际上是 DTE 和 DCE 或其他通信设备之间的一组约定，主要解决网络节点与物理信道如何连接的问题。其中 DTE（Data Terminal Equipment）是指数据终端设备，如数据输入、输出设备和传输控制器或计算机等数据处理装置及其通信控制器，它的基本功能是产生、处理数据；DCE（Data Circuit-terminal Equipment）是指数据电路端接设备，如自动呼叫设备、调制解调器及其他一些中间装置的集合，它的功能是发送、接收数据。

DTE 与 DCE 之间要连接，必须遵循共同的接口标准。该接口标准主要有 4 个方面的特性：

（1）机械特性：该特性规定了连接时所采用的可接插连接器的规格和尺寸、连接器中引脚的数目和排列情况等。

（2）电气特性：该特性规定了在物理连接上传输二进制比特流时，线路上信号电压的高低、传输速率和距离的限制等。

（3）功能特性：功能特性规定各信号线的功能或作用。信号线按功能可分为数据线、控制线、定时线和接地线等。

（4）规程特性：规程特性定义 DTE 和 DCE 通过接口连接时，各信号线进行二进制位流传输的一组操作规程（动作序列），如怎样建立、维持和拆除物理连接，全双工还是半双工操作等。

### 3．物理层的网络连接设备

（1）中继器

信号在通过物理介质传输时或多或少会受到干扰、产生衰减。如果信号衰减到一定的程度，信号将不能识别。因此，采用不同传输介质的网络对网线的最大传输距离都有规定。例如：同轴电缆构建的粗缆以太网的最大电缆长度为 50m，非屏蔽双绞线构建 100Base-T 以太网的最大电缆长度为 100m。如果要延伸网络信号的传输距离，就需要安装一个称为“中继器”的设备。

中继器工作在 OSI 参考模型的物理层上，其功能是对衰减的信号进行再生和放大（如图 1-4）。由于中继器在网络数据传输中起到了放大信号的作用，因此可以“延长”网络的距离。

中继器的主要优点是安装简单、使用方便、价格相对低廉。它不仅起到扩展网络距离的作用，还可以连接不同传输介质的网络。

（2）集线器 Hub

集线器具有多个端口，不仅用于集中网络连接，还可以重发数字信号。局域网中最常用的是连接以太网的 Hub。其他类型的 Hub 包括用于令牌环网络的多站访问单元（MAU），见第 4 章的相关介绍。

集线器具有与中继器相似的信号中继和放大特性，因而被称为多端口中继器。两者的主要区别是：中继器一般为两个端口，一个端口接收数据，另一个端口进行放大转发；而集线器具有多个端口（8 口、16 口和 24 口等），数据到达一个端口后，将被转发到其他所有端口（广播）。所以图 1-5 所示用 Hub 连接的网络是物理上星形而逻辑上是总线形的拓扑结构。集线器有多种分类方法：

① 依据带宽的不同，集线器分为 10Mbps、100Mbps、10/100Mbps 自适应、1 000Mbps、100/1 000Mbps 自适应等，小型局域网通常使用前 3 种。

② 按配置形式的不同可分为独立型集线器、模块化集线器和堆叠式集线器。

③ 根据管理方式又可分为智能型集线器和非智能型集线器。所谓智能型 Hub 除了具有 Hub 的基本功能外，还具有 SNMP（Small Network Management Protocol）网管功能。

目前所使用的集线器基本是以上 3 种分类的组合。例如，10/100Mbps 自适应智能型可堆叠式集线器。

### 3.2.3　数据链路层

#### 1．数据链路层的功能

数据链路层的作用是对物理层传输原始比特流的功能的加强，它将物理层提供的可能出错的物理连接改造成为逻辑上无差错的数据链路，即使之对网络层表现为一条无差错的数据链路。因此，数据链路层的主要任务就是对传输操作进行严格的控制和管理，检测并纠正物理层传输介质上产生的传输差错。数据链路层的信息传输单位是帧（Frame），它包含足够的信息，确保数据可以安全地通过本地局域网到达目的地。成功发送意味着数据帧要完整无缺地到达目的地。也就是说，帧中必须包含一种机制用于保证在传送过程中内容的完整性。有很多情况可以导致帧的发送不能到达目标或者在传输过程中被破坏或不能使用，数据链路层有责任检测并修正所有这些错误。数据链路层的功能如下：

（1）数据链路的管理

链路两端的节点在进行通信前，必须确认对方已进入就绪状态，并交换一些必要的信息以对帧进行初始化，然后再建立链路的连接，在传输过程中还要维持这种连接，传输完毕要拆除该连接。

（2）帧同步

帧是数据链路层传输的数据单位。每个帧包括帧头、帧尾、帧检验码和帧序号。帧头和帧尾用以表示帧的开始和结束，接收方要能从物理层收到的比特流中明确区分出一帧的开始和结束，这就是帧同步。

（3）差错控制

差错控制是指在数据通信过程中发现能检测或纠正差错，并将差错限制在尽可能小的允许范围内。差错检测可通过差错控制编码来实现；而差错纠正则通过差错控制方法来实现。详见“差错控制技术”一节中的相关介绍。

（4）流量控制

如果发送节点的发送能力大于接收节点的接收能力，将导致接收方来不及接收。流量控制所要解决的就是控制发送方的速率，使其不超过接收方所能承受的能力。

### 2．数据链路层协议和高级数据链路控制协议（HDLC）

（1）数据链路层协议分类

数据链路控制协议可分为异步协议和同步协议两类。

异步协议以字符为独立的信息传输单位，在每个字符的起始处对字符内的比特实现同步，但字符与字符之间的间隔时间是不固定的（即字符之间是异步的）。由于每个传输字符都要添加诸如起始位、校验位、停止位等冗余位，故信道利用率很低，一般用于数据速率较低的场合。

同步协议是以许多字符或许多比特组织成的数据块——帧为传输单位，在帧的起始处同步，使帧内维持固定的时钟。由于采用帧为传输单位，所以同步协议能更有效地利用信道，也便于实现差错控制、流量控制等功能。同步协议又可分为面向字节计数的同步协议、面向字符的同步协议和面向比特的同步协议。其中，面向比特的同步协议的典型代表是 HDLC（High-level Data Link Control）。

HDLC 协议的特点是：不依赖于任何一种字符编码集，实现透明传输的“0 比特插入/删除法”易于硬件实现；全双工通信，不必等待确认便可连续发送数据，有较高的数据链路传输效率；所有帧均采用 CRC 校验；对信息帧进行顺序编号，可防止漏收或重发，传输可靠性高等。

（2）HDLC 帧格式简介

HDLC 帧由标志字段（F）、地址字段（A）、控制字段（C）、信息字段（I）和帧校验序列字段（FCS）组成，如表 3-1 所示。

表 3-1　HDLC 帧格式

| F | A | C | I | FCS | F |
|---|---|---|---|---|---|
| 01111110 | 8 位 | 8 位 | 可变长度 | 16 位 | 01111110 |

其中：

① 标志字段 01111110 用以标志帧的起始和前一帧的终止。

② 地址字段的内容取决于所采用的操作方式。命令帧中的地址字段携带的是相邻结点的地址，而响应帧中的地址字段携带的是本节点地址。

③ 控制字段通过不同编码构成各种命令和响应，以便对链路进行监视和控制。该字段是 HDLC 协议的关键部分。

④ 信息字段用于传送有效数据，下限可以为 0（无信息字段），上限未做严格限定，但实际上要受 FCS 字段或站点缓冲器容量的限制，一般是 1 000～2 000 比特。

⑤ 帧校验序列字段可以使用 16 位或 32 位的 CRC，对两个标志字段之间的整个帧的内容进行校验。有关 CRC 的工作原理见“差错控制编码”中的相关介绍。

### 3．数据链路层的网络连接设备

（1）网卡

网卡又称网络接口卡，是主机与网络的接口部件。网卡是一种能发出和接收数据帧、计算帧检验序列、执行编码译码转换等以实现网络节点间数据交换的集成电路卡。网卡上有收发器、介质访问控制逻辑和设备接口，主要完成以下功能：控制数据传送、具备串-并转换功能、缓存功能。

每块网卡都有一个 MAC 地址。网卡初始化后，该网卡的 MAC 将载入设备的 RAM 中。例如，执行 DOS 命令：ipconfig/all，可获知本机网卡的 MAC。

MAC 地址是全球唯一的物理地址，由厂家在生产时固化到网卡的 ROM 中。MAC 地址的前 6 个十六进制数字表示制造商或厂商编号，后 6 个十六进制数字表示 NIC 序号。

网卡按总线类型可分为 ELSA 网卡、ISA 网卡、PCI 网卡、PCMCIA 网卡和 USB 网卡等；按传输速率可分为 10Mbps 网卡、100Mbps 网卡、10/100Mbps 自适应网卡以及千兆网卡等。

（2）网桥（Bridge）

网桥又称为桥接器，用于分隔网络。一个网络的物理连线距离虽然在规定范围内，如果负荷很重，可用网桥把它分隔成两部分，即分成网段 1 和网段 2。

网桥仅是基于 MAC 地址来过滤网络流量的，它与上面运行什么网络层协议无关，即网桥对网络层以上的协议是完全透明的。网桥通常用于连接同一类型的网络（物理层可以不同，例如，可连接使用 UTP 的以太网与使用同轴电缆的以太网）。

网桥的工作原理是依据 MAC 地址和网桥路由表实现帧的路径选择。网桥刚启动时，这个路由表是空的，当某一节点传送的数据通过网桥时，如果该 MAC 地址不在路由表中，网桥会自动记下其地址及对应的网桥端口号。通过这样一个“学习”过程，可建立起一张完整的网桥路由表。

（3）交换机

交换机也称为交换式集线器，是一个由许多高速端口组成的设备。

交换机实际上是由网桥发展而来的，工作原理与网桥相似。在交换机内存中建立起一张 MAC 地址和端口号的关联表。交换机根据所传送的数据帧的目的地址，将每个数据帧独立地从源端口送至目的端口，不会影响其他端口。因此，交换机通过在端口间创建的临时逻辑连接，可以同时互不影响的传送多路数据帧，得到几倍于常规 LAN 带宽的网络效应，提高了网络的实际吞吐量，使得整个网络的带宽得到最大化地利用。

交换机从外表上看与 Hub 非常相似，区别在于：交换机基于 MAC 地址向特定端口转发数据帧，而 Hub 是向所有端口广播发送数据帧；前者是独享带宽，后者是共享带宽。例如，有一台 100Mbps 的 Hub，连接了 $N$ 台主机，则 $N$ 台主机共享 100Mbps 带宽，每台主机所分配到的带宽只有 100Mbps/$N$；而对于一台 100Mbps 的交换机，每个端口的带宽均为 100Mbps，即每台连接的主机均可获得 100Mbps 带宽。

### 3.2.4 网络层

#### 1．网络层的功能

网络层是 OSI 参考模型的第 3 层，又称为通信子网层，是计算机网络中的通信子网与网络高层的接口（由于通信子网不存在路由选择问题），在数据链路层提供服务的基础上向资源子网提供服务。网络层负责在源节点和目标节点之间建立它们所使用的路由。这一层本身没有任何错误检测和修正机制，因此网络层必须依赖数据链路层提供的可靠传输。

概括地说，网络层主要有以下功能：

（1）为传输层提供服务

网络层提供的服务有两类：面向连接的网络服务和无连接的网络服务。其中面向连接的网络服务又称虚电路服务，它分为连接建立、数据传输和连接释放 3 个阶段，是网络层向运输层提供的一种可靠的数据传送方式，所有分组按照发送顺序到达。进行数据交换的两个端系统之间有一条虚电路（网络连接）为它们服务；而无连接的网络服务又称为数据报服务。这种服务在两个实体之间进行通信时，不需要事先建立好一个连接，即没有连接建立和连接释放的过程，源节点发送的每个数据包都要附加地址、序号等信息，目的节点收到的数据包不一定按序到达，还可能出现数据包的丢失现象。故称为无连接的不可靠的服务。

典型的网络层协议是 X.25，它是由 ITU-T（国际电信联盟电信标准部）提出的一种面向连接的分组交换协议。

（2）组包和拆包

在网络层，数据传输的基本单位是数据包（也称为分组）。在发送方，传输层的报文到达网络层时被分为多个数据块，在这些数据块的头部和尾部加上一些相关控制信息后，即组成了数据包（组包）。数据包的头部包含源节点和目标节点的网络地址（逻辑地址）。在接收方，数据从低层到达网络层时，要将各数据包原来加上的包头和包尾等控制信息去掉（拆包），然后组合成报文，送给传输层。

（3）路由选择

路由选择也叫做路径选择，是根据一定的原则和路由选择算法在多节点的通信子网中选择一条最佳路径。确定路由选择的策略称为路由算法。

在数据报方式中，网络节点要为每个数据包做出路由选择；而在虚电路方式中，只需在建立连接时确定路由。

（4）流量控制

流量控制的作用是控制阻塞，避免死锁。

网络的吞吐量（数据包数量/秒）与通信子网负荷（即通信子网中正在传输的数据包数量）有着密切的关系。对防止出现阻塞和死锁，需要进行流量控制，通常可采用滑动窗口、预约缓冲区、许可证和分组丢弃 4 种方法。

#### 2．路由选择算法简介

路由算法有很多，大致可分为静态路由选择算法和动态路由选择算法两类。

静态路由选择算法又称为非自适应算法，是按某种固定规则进行的路由选择。其特点是

算法简单、容易实现，但效率和性能较差。属于静态路由选择算法的有：最短路由选择算法、扩散式路由选择算法、随机路由选择算法、集中路由选择算法。动态路由选择算法又称为自适应算法，是一种依靠网络的当前状态信息来进行的路由选择。其特点是能较好地适应网络流量、拓扑结构的变化，网络性能得到改善，但算法复杂，实现开销大。属于动态路由选择算法的有：分布式路由选择算法、集中路由选择算法等。

#### 3．网络层的网络连接设备

（1）路由器

在互联网中，两台主机之间传送数据的通路会有很多条，数据包从一台主机出发，中途要经过多个站点才能到达另一台主机。这些中间站点通常由称为路由器的设备担当，其作用就是为数据包选择一条合适的传送路径。

路由器工作在 OSI 模型的网络层，是根据数据包中的逻辑地址（网络地址）而不是 MAC 地址来转发数据包的。它的主要工作是为经过路由器的每个数据包寻找一条最佳传输路径，并将该数据包有效地传送到目的站点。路由器不仅有网桥的全部功能，还具有路径的选择功能，可根据网络的拥塞程度，自动选择适当的路径传送数据。

路由器与网桥的不同之处在于：它并不是使用路由表来找到其他网络中指定设备的地址，而是依靠其他的路由器来完成任务的。也就是说，网桥是根据路由表来转发或过滤数据包，而路由器是使用它的信息来为每一个数据包选择最佳路径。

路由器有静态和动态之分。静态路由器需要管理员来修改所有的网络路由表，一般只用于小型的网络间互连；而动态路由器能根据指定的路由协议来完成修改路由器信息。

（2）第三层交换机

随着技术的发展，有些交换机也具备了路由的功能。这些具有路由功能的交换机要在网络层对数据包进行操作，因此被称为第三层交换机。

### 3.2.5　传输层

#### 1．传输层的地位和作用

在 OSI 的七层模型中，低三层是面向数据通信的，是由通信子网所完成的通信功能的集合，通信子网就是基于低三层通信协议构成的网络；高三层是由端主机进程所完成的面向应用功能的集合。传输层在 OSI 的七层模型中恰好处于正中间。是高层与低层之间的接口层，因此传输层起承上启下的作用，是计算机网络中的资源子网和通信子网的接口和桥梁，对于网络中通信的两个主机，其端到端的可靠通信最后要靠传输层来完成。

传输层是 OSI 中负责通信的最高层，传输层还是 OSI 中用户功能的最低层。传输层及以上各层的数据传输单位均为报文。传输层的任务是在网络层提供的网络连接基础上，补充和完善通信子网的服务，为源主机和目的主机进程之间提供可靠的、端到端数据的透明传输。

网络层向传输层提供的有面向连接的可靠的服务和无连接的不可靠的服务两类，但传输层对高层来说，它屏蔽掉了通信子网的具体操作，提供的是端到端的可靠通信。如果通信子网功能完善，那么传输层的任务就比较简单。如果通信子网质量很差，那么传输层就必须弥补和加强网络层提供的服务。

### 2．传输层的功能

（1）分割与重组数据

在发送方，传输层将会话层发来的数据分割成较小的数据单元，并在这些数据单元的头部加上一些相关控制信息后，形成段或报文，报文的头部包含源端口号和目标端口号。在接收方，数据经通信子网到达传输层时，要将各报文原来加上的报文头等控制信息去掉（拆包），然后按照正确的顺序进行重组，恢复原来的数据，送给会话层。

（2）按端口号寻址

端口是与网络地址对应的，但是同一端点上可能有许多个应用程序进程，它们在同一时间内都在进行通信。例如，一个用户正在进行向某一服务器上传文件的进程，另一个用户则可能正在使用该服务器的邮件服务。传输层通过端口号寻址端点上的进程，并使用多路复用技术处理多端口同时通信的问题。

（3）连接管理

面向连接的传输服务要负责建立、维持和释放连接。典型的连接是通过“三次”握手实现的。

（4）差错控制和流量控制

传输层要向会话层提供通信服务的可靠性，避免报文的出错、丢失、延迟时间紊乱、重复、乱序等差错。因此要提供端到端的差错控制：通过这一层传输的数据将由目标端点进行确认，如果在指定的时间内未收到确认信息，源端点将重发数据。此外，为了避免接收方缓冲区溢出，传输层还具有流量控制的作用，以控制发送端口的速率，使其不超过接收端口所能承受的能力。窗口技术是常用的流量控制方法。

### 3．传输层的网络服务质量与协议等级

（1）网络服务质量

根据提供的服务质量的不同，传输层的网络服务可分为以下 3 种类型：

① A 类服务：低差错率连接，即具有可接受的残留差错率和故障告知率。

② C 类服务：高差错率连接，即具有不可接受的残留差错率和故障告知率。

③ B 类服务：介于 A 类服务与 C 类服务之间。

（2）协议等级

差错率的接受与不可接受是取决于用户的。因此，网络服务质量的划分是以用户要求为依据的。OSI 根据传输层的功能特点，定义了以下 5 种协议级别：

① 0 级：简单连接。只建立一个简单的端到端的传输连接，并可分段传输长报文。

② 1 级：基本差错恢复级。在网络连接断开、网络连接失败或收到一个未被认可的传输连接数据单元等基本差错时，具有恢复功能。

③ 2 级：多路复用。允许多条传输共享同一网络连接，并具有相应的流量控制功能。

④ 3 级：差错恢复和多路复用。是 1 级和 2 级协议的综合。

⑤ 4 级：差错检测、恢复和多路复用。在 3 级协议的基础上增加了差错检测功能。

（3）典型的传输层协议

① SPX 协议：顺序包交换协议，是 Novell NetWare 网络的传输层协议。

② TCP 协议：传输控制协议，是 TCP/IP 参考模型的传输层协议。

### 3.2.6　网络高层

会话层、表示层和应用层一起构成 OSI 参考模型的高层。与低层不同的是：高层主要考虑面向用户的服务，低层主要涉及提供可靠的端到端通信。

#### 1．会话层

会话层的功能主要是在传输层所提供的服务的基础上，组织和同步进程间的通信，提供会话服务、会话管理和会话同步等功能。所谓的“会话”指的是本地系统的会话实体与远程实体之间交换数据的过程。

会话层不参与具体的数据传输，仅提供包括访问验证和会话管理在内的建立和维护应用程序间通信的机制，如服务器验证用户登录便是由会话层完成的。

（1）会话服务

会话层服务包括会话连接管理服务、会话数据交换服务、会话交互管理服务、会话连接同步服务和异常报告服务等。会话服务过程可分为会话连接建立、报文传送和会话连接释放 3 个阶段。

（2）会话控制

从原理上说，OSI 中的所有连接都是全双工的。

会话层通过令牌来进行会话的交互控制。令牌是会话连接的一个属性，表示使用会话的独占权：拥有令牌的一方才有权发送数据。令牌是可以申请的，各个端系统对令牌的使用权可以具有不同的优先级。

（3）会话同步

所谓同步就是使会话服务用户对会话的进展情况都有一致的了解，在会话被中断后可以从中断处继续下去，而不必从头恢复会话。

会话层定义的同步点有主同步点和次同步点两类。主同步点用于每个会话单元，次同步点用于单元内的同步控制。

#### 2．表示层

表示层主要解决的是信息以什么样的表现形式（数据表现）传送给对方，不关心处理的用户数据有什么样的意义，只考虑用什么样的传送形式传送这一问题。也就是说表示层的功能并不是信息的具体表达，而是处理信息表示中所遇到的问题，考虑如何将不同信息的表达形式转换成公共的信息传送形式。表示层向应用层主要提供如下服务：

（1）数据表示

解决数据的语法表示问题，如文本、声音、图形图像的表示，即确定数据传输时的数据结构。

（2）语法转换

为使各个系统间交换的数据具有相同的语义，应用层采用的是对数据进行一般结构描述的抽象语法，如使用 ISO 提出的抽象语法标记 ASN.1。表示层为抽象语法指定一种编码规则，便构成一种传输语法。语法转换就是把抽象语法与传输语法按照一定的规则相互转换的过程。

发送方把自己的抽象语法转换成传输语法，接收方收到数据后，再把传输语法转换为自己的局部语法。

（3）语法选择

传输语法与抽象语法之间是多对多的关系，即一种传输语法可对应于多种抽象语法，而一种抽象语法也可对应于多种传输语法。所以传输层应能根据应用层的要求，选择合适的传输语法传送数据。

（4）连接管理

利用会话层提供的服务建立表示连接，并管理在这个连接之上的数据传输和同步控制，以及正常或异常地终止这个连接。

3．应用层

在 OSI 参考模型的最顶层，它是计算机网络与最终用户间的接口，它包括了系统管理员管理网络服务所涉及的所有问题和基本功能。它在 OSI 参考模型下面六层提供的数据传输和数据表示等各种服务的基础上，为网络用户或应用程序提供完成特定网络服务功能所需的各种应用协议。常用的网络服务包括文件服务、邮件服务、打印服务、网络管理服务、安全服务、多协议路由与路由互连服务、分布式数据库服务，以及虚拟终端服务等。

## 3.3　TCP/IP 参考模型

### 3.3.1　TCP/IP 概述

TCP/IP（Transmission Control Protocol/Internet Protocol）是指传输控制协议 / 网际协议。它起源于美国的 ARPANET 网，由它的两个主要协议即 TCP 协议和 IP 协议而得名。TCP/IP 是 Internet 上所有网络和主机之间进行交流所使用的共同“语言”，是 Internet 上使用的一组完整的标准网络协议。通常所说的 TCP/IP 协议实际上包含了大量的协议和应用，且由多个独立定义的协议组合在一起，因此，更确切地说，应该称其为 TCP/IP 协议集。

OSI 参考模型研究的初衷是希望为网络体系结构与协议的发展提供一种国际标准，但由于 Internet 在全世界的飞速发展，使得 TCP/IP 协议得到了广泛的发展，虽然 TCP/IP 不是 ISO 标准，但广泛的使用也使 TCP/IP 成为一种“实际上的标准”，并形成了 TCP/IP 参考模型。不过 ISO 的 OSI 参考模型的制定也参考了 TCP/IP 协议集及其分层体系结构的思想。而 TCP/IP 在不断的发展过程中也吸收了 OSI 标准中的概念及特征。

与 OSI 参考模型不同，TCP/IP 参考模型更侧重于互连设备间的数据传送，而不是严格的功能层次划分。它通过解释功能层次分布的重要性来做到这一点，但它仍为设计者具体实现协议留下很大的余地。又因为 TCP/IP 是 Internet 采用的协议标准。Internet 的迅速发展和普及，使得 TCP/IP 协议成为全世界计算机网络中使用最广泛、最成熟的网络协议，它同样也适用于在一个局域网中实现异种机的互连通信。

### 3.3.2　TCP/IP 体系结构中各层的功能

TCP/IP 虽不是国际标准，但它也是为全世界广大用户和厂商接受的网络互连的事实标准。TCP/IP 参考模型也是一种分层网络体系结构。基于 TCP/IP 协议的网络体系结构与 OSI 参考模型相比，结构更简单，其参考模型如图 3-4 所示。TCP/IP 协议的网络体系结构分为 4 个层次，分别是网络接口层、网络互连层、传输层和应用层。

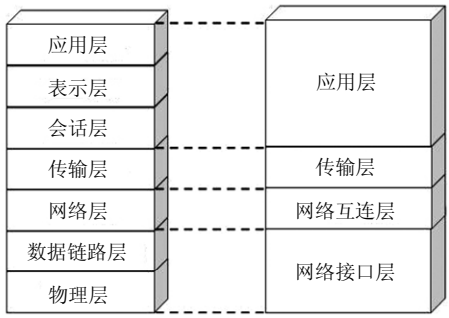



图 3-4　TCP/IP 参考模型与 OSI 参考模型

各层的功能如下：

#### 1．网络接口层

在 TCP/IP 参考模型中，网络接口层是参考模型的最低层，它负责通过网络发送和接收 IP 数据报。TCP/IP 参考模型允许主机接入网络时使用多种现成的或流行的协议，这使得 TCP/IP 协议可以运行在底层网络上，以便实现它们之间的相互通信。网络接口层对高层屏蔽了底层物理网络的细节，是 TCP/IP 成为互联网际协议的基础。

#### 2．网络互连层

在 TCP/IP 参考模型中，网络互连层是参考模型的第二层，相当于 OSI 参考模型的网络层。网络互联层的主要功能如下：

① 接收到分组发送请求后，将分组装入 IP 数据报，填充报头并选择发送路径，然后发送到相应的网络输出线。

② 接收到其他主机发送的数据报后，检查目的地址，如果需要转发，则选择发送路径，转发出去。如果目的地址为本节点 IP 地址，则除去报头，将分组交送传输层处理。

③ 处理网络互连的路径选择、流量控制和拥塞控制问题。

在网络互连层中，最常用的协议是 IP 协议，还有 ARP、RARP 和 ICMP 一系列路由协议。

（1）IP 协议

IP 协议是 Internet 的基本协议，它把传输层送来的信息组成 IP 数据报，并把 IP 数据报传递给网络接口层。IP 提供不可靠的、无连接的数据报传递服务。所谓不可靠，是指不能保证正确传送，分组可能丢失、重复、延迟或不按顺序传送，既不验证，也不发确认，只是将分组尽量传送到目的地。

IP 协议提供如下功能：

① IP 地址寻址。指出发送和接收 IP 数据报的源 IP 地址及目的 IP 地址。

IP 地址是 32 位的逻辑地址，被分成 4 段，每段 8 位（1 字节）。IP 地址通常用十进制形式表示，每段由 0～255 的数字组成，段与段之间用小数点分隔，例如：192.168.1.100。一个 IP 地址可唯一地标识出网络上的每个主机。详见第 5 章有关 IP 地址的介绍。

② IP 数据报的分段与重组。不同网络的数据链路层可传输的数据帧的最大长度不一样。因此，IP 协议要能根据不同情况，对数据报进行分段封装，使得很大的 IP 数据报能以较小的分组在网上传输。更确切地说，IP 协议和网络接口层之间传送的数据单元应该是分组。分组既可以是一个 IP 数据报，也可以是 IP 数据报的一个分段。

目的主机上的 IP 协议能根据 IP 数据报中的分段与重组标识，将各个 IP 数据报分段重新组装为原来的数据报，然后交给上层协议。

③ IP 数据报的路由转发。根据 IP 数据报中接收方的目的 IP 地址，确定是本网传送还是跨网传送。若目的主机在本网中，可在本网中将数据报传给目的主机；若目的主机在别的网络中，则通过路由器将数据报转发到另一个网络或下一个路由器，直至转发到目的主机所在的网络。

（2）ICMP 协议

由于 IP 协议提供的是一种不可靠的和无连接的数据报服务，为了对 IP 数据报的传送进行差错控制，对未能完成传送的数据报给出出错的原因，TCP/IP 协议簇在网络互连层提供了一个用于传递控制报文的 ICMP 协议，即互联网控制报文协议。

ICMP 协议允许路由器或目的主机提供有关差错和异常情况的报文。常用的检查网络连通性的 Ping 命令，其过程实际上就是 ICMP 协议工作的过程。

ICMP 协议必须在 IP 协议的基础上进行工作，因为 ICMP 传递的控制报文是作为 IP 数据报的数据部分进行封装，即以 IP 数据报的形式进行传送。因此，无法保证 ICMP 报文不会被丢失或丢弃。

（3）地址解析协议 ARP 和逆向地址解析协议 RARP

在 TCP/IP 环境中，每个主机的 32 位 IP 地址只是一个逻辑地址，在传送时必须转换成物理地址，也称为 MAC 地址。因此需要一种能将 IP 地址转换为 MAC 地址的协议，ARP 就是这样一种地址解析协议。

ARP 的解析过程是：在进行数据报发送时，源主机先在其 ARP 缓存表中查看有无目的主机的 IP 地址，若有，可获得相应的 MAC 地址；若没有，则通过广播 ARP 请求的方式查找目的主机的 MAC 地址，并将获得的信息写入源主机的 ARP 缓存表。ARP 缓存表里的 IP 地址与 MAC 地址是一一对应的。例如，在安装 TCP/IP 协议的联网主机中执行 DOS 命令：arp –a，可获得本机 ARP 缓存表的内容。

逆向地址解析协议 RARP 用于从物理地址到 IP 地址的转换。一个网络设备或工作站可能知道自己的 MAC 地址，但是不知道自己的 IP 地址。设备发送 RARP 请求，网络中的一个 RARP 服务器来应答 RARP 请求，RARP 服务器有一个事先做好的从工作站硬件地址到 IP 地址的映射表，当收到 RARP 请求分组后，RARP 服务器就从这张映射表中查出该工作站的 IP 地址，然后写入 RARP 响应分组，发回给工作站。

### 3．传输层

在 TCP/IP 参考模型中，传输层是参考模型的第三层，它负责在应用进程之间的端－端通信。传输层的主要作用是：在互联网中源主机与目的主机间建立用于会话的端－端连接。TCP/IP 参考模型的传输层与 OSI 参考模型的传输层功能是相似的。

TCP/IP 体系结构的传输层定义了传输控制协议 TCP（Transport Control Protocol）和用户数据报协议 UDP（User Datagram Protocol）两种协议。

TCP 协议提供端到端的面向连接的服务，提供全双工的、可靠的、有流量控制的字节流服务。即 TCP 将这些字节缓冲，分段交给 IP 协议。可靠服务是指数据有保证地传递、按序、没有重复。为取得可靠的传送，TCP 必须检测分组丢失，收不到确认时自动重传，处理延迟的重复数据报等许多操作。TCP 协议的主要功能是：

① 确保数据报的成功传递；

② 对程序发送的大的数据进行分段和重组；

③ 确保正确排序以及按顺序传递分段的数据；

④ 进行传输数据的完整性检查。

UDP 协议是一个无连接服务的协议。它提供不可靠的数据传输服务，这就意味着 UDP 无法保证数据的正确传送或验证数据的顺序。因此，UDP 报文可能会出现丢失、重复或乱序到达的现象。

尽管 UDP 提供的是不可靠的服务，但是它开销小、效率高，因而适用于速度要求高而功能简单的类似请求 / 响应方式的数据通信。

### 4．应用层

在 TCP/IP 体系结构中，传输层之上是应用层。它包括了所有的高层协议，并且总是不断有新的协议加入，其主要协议包括：

（1）远程终端协议（Telnet）：实现互联网中远程登录功能。

（2）文件传输协议 FTP（File Transfer Protocol）：用于实现互联网中的交互式文件传输功能。

（3）简单邮件传输协议 SMTP（Simple Mail Transfer Protocol）：实现互联网中电子邮件的传送功能。

（4）域名系统 DNS（Domain Name System）：实现网络设备名字到 IP 地址映射的网络服务。

（5）简单网络管理协议 SNMP（Simple Network Management Protocol）：管理与监视网络设备。

（6）超文本传输协议 HTTP（Hypertext Transfer Protocol）：用于 WWW 服务。

（7）路由信息协议 RIP（Routing Information Protocol）：在网络设备（路由器）之间交换路由信息。

应用层协议主要分 3 类：一类是依赖于面向连接的 TCP 协议；一类是依赖于面向无连接的 UDP 协议；另一类是既依赖于 TCP 协议，也可依赖于 UDP 协议。其中依赖 TCP 协议的主要有网络终端协议、电子邮件协议、文件传输协议等；依赖 UDP 协议的主要有简单网络管理协议、简单文件传输协议等；既可依赖于 TCP 协议又可依赖于 UDP 协议的主要有域名系统等。

### 3.3.3 OSI 参考模型与 TCP/IP 参考模型的比较

**1．相似之处**

二者都采用层次结构模型，在某些层次上有着相似的功能。

OSI 参考模型是国际标准化组织 ISO 制定的一个国际标准，但它并没有成为事实上的国际标准；而 TCP/IP 不是国际标准，却成为了事实上的工业标准。二者分别作为概念上的模型和事实上的标准，具有同等的重要性。

**2．不同之处**

（1）OSI 参考模型采用了 7 层体系结构，而 TCP/IP 参考模型采用了 4 层体系结构。虽然它们具有功能相当的网络层、传输层和应用层，但其他层并不相同。

TCP/IP 模型中没有专门的表示层和会话层，它将这两层相关的功能包含到了应用层中去完成。另外，TCP/IP 模型还将 OSI 的数据链路层和物理层包括到了网络接口层中。

（2）OSI 参考模型在网络层支持无连接和面向连接的两种服务，而在传输层仅支持面向连接的服务。TCP/IP 在网络层则支持无连接的一种服务，但在传输层支持面向连接和无连接两种服务。

（3）TCP/IP 模型有较少的层次，显得比较简单，TCP/IP 一开始就考虑到多种异构网络互连问题，并将网际协议（IP）作为 TCP/IP 的重要组成部分，并且作为从 Internet 上发展起来的协议，已经成为网络互连的事实标准。但是，目前还没有实际网络是建立在 OSI 模型基础上的，OSI 仅作为理论的参考模型被广泛使用。

尽管 OSI 参考模型存在着不足之处，但其模型的层次划分以及内容却是值得肯定的。也许正是大而全和层次划分的复杂性，才使得人们只要了解和掌握了 OSI 参考模型，就能对网络体系结构的概念、结构、功能以及层间关系有一个明确的概念。而且 OSI 参考模型的层次划分及功能也可很方便地套用到其他网络体系结构的层次分析上。如 TCP/IP、LAN 参考模型都可通过对照 OSI 的层次划分和功能，得以清晰解释。OSI 参考模型对计算机网络的发展，尤其是对网络体系结构的发展有着很高的指导意义和学术价值。因此将 OSI 参考模型作为网络理论的研究基础和计算机网络教学的理论模型，对于计算机网络的教学是十分有益的。

## 练习 3

**一、填空题**

（1）网络协议一般是由_____、_____和_____3 要素组成。

（2）OSI 参考模型将整个网络分为 7 层（自高到低）分别是_____、_____、_____、_____、_____、_____和_____。

（3）OSI 参考模型中物理层协议包括_____、_____、_____和_____4 个方面的内容。

（4）连接设备的物理接口包含_____、_____、_____和

_____4 个方面的特性。

（5）在 OSI 框架结构中，第 *N* 层实体与对等层之间使用_____进行协商，还通过层间的_____使用来自第_____层的服务，并为第_____层提供服务。

## 二、选择题

（1）下面选项中说法是正确的（　　）。

A．物理层的数据单元是二进制的比特流

B．物理层是 OSI/RM 中的第一层，而传输介质是第零层

C．物理层的功能是将一条有差错的物理链路改造成无差错的数据链路

D．以上说法都不对

（2）下面哪一个选项不是协议的三要素（　　）。

A．语法　　B．语义　　C．服务　　D．定时

（3）关于 OSI 的体系结构，下面哪个说法是正确的（　　）。

A．OSI 的体系结构定义了一个七层模型，用以进行进程间的通信

B．OSI 的体系结构定义描述了各层所提供的服务

C．OSI 的体系结构定义了应当发送何种控制信息及解释该控制信息的过程

D．以上说法都不对

（4）下面哪一个不是数据链路层的功能（　　）。

A．链路管理　　B．帧同步　　C．差错控制　　D．路由选择

（5）数据报服务是（　　）。

A．面向连接的、可靠的、保证分组顺序到达的网络服务

B．无连接的、不可靠的、不保证分组顺序到达的网络服务

C．面向连接的、不可靠的、保证分组顺序到达的网络服务

D．无连接的、可靠的、保证分组顺序到达的网络服务

## 三、简答题

（1）什么叫分层网络体系结构？OSI 参考模型将计算机网络体系结构共分成几层？每层传送的数据单元分别是什么？

（2）画出 OSI 的层次结构，并简述各层的功能。

（3）简述物理层的功能，并说明物理层接口的主要特征。

（4）HDLC 的帧格式如何？各字段的含义是什么？

（5）网络层的主要功能是什么？

（6）集线器与中继器有何异同？交换机与集线器又有何异同？路由器与网桥的不同之处呢？试举例加以说明。

（7）试比较 OSI 参考模型与 TCP/IP 模型的异同。

（8）简述网络中两台主机之间通信时，数据的传输方式。

# 第4章

# 局域网技术

局域网是计算机网络的重要组成部分，是当今计算机网络技术应用与发展非常活跃的一个领域。公司、企业、政府部门及住宅小区内的计算机都通过 LAN（局域网）连接起来，以达到资源共享、信息传递和数据通信的目的。而信息化进程的加快，更是刺激了通过 LAN 进行网络互连需求的剧增。因此，理解和掌握局域网技术也就显得很重要。

通过本章的学习，应达到如下学习目标：

（1）了解局域网的基本概念和工作原理、局域网的体系结构及 IEEE 802.x 系列局域网标准；

（2）熟悉各种局域网技术，了解最新局域网技术的发展；

（3）掌握局域网的组网技术；

（4）具有一定的独立设计、组建局域网能力。

## 4.1 局域网概述

局域网（Local Area Network，LAN）是应用最为广泛的一类网络，它是将较小地理范围内的各种数据通信设备连接在一起的计算机网络，常常位于一个建筑物或一个园区内，也可以远到几千米的范围。局域网通常用来将单位办公室中的个人计算机和办公设备连接起来，以便共享资源和交换信息，它是专有网络。

局域网的发展始于 20 世纪 70 年代，至今仍是网络发展中的一个活跃领域。到了 20 世纪 90 年代，LAN 更是在速度、带宽等指标方面有了更大进展，并且在 LAN 的访问、服务、管理、安全和保密等方面都有了进一步的改善。例如，Ethernet 技术从传输速率为 10Mbps 发展到 100Mbps 的高速以太网，并继续提高至千兆位（1 000Mbps）以太网、万兆位以太网。

### 4.1.1 局域网的特点

局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。局域网具有如下特点：

① 网络所覆盖的地理范围比较小。通常不超过几十千米，甚至只在一个园区、一幢建筑或一个房间内。

② 数据的传输速率比较高，从最初的 1Mbps 到后来的 10Mbps、100Mbps，近年来已达

到 1 000Mbps、10 000Mbps。

③ 具有较低的延迟和误码率，其误码率一般为 10.8～10.11。

④ 局域网络的经营权和管理权属于某个单位所有，与广域网通常由服务提供商提供形成鲜明对照。

⑤ 便于安装、维护和扩充，建网成本低、周期短。

尽管局域网地理覆盖范围小，但这并不意味着它们必定是小型的或简单的网络。局域网可以扩展得相当大或者非常复杂，配有成千上万用户的局域网也是很常见的事。局域网具有如下的一些优点：

① 能方便地共享昂贵的外部设备、主机以及软件、数据，从一个站点可访问全网。

② 便于系统的扩展和逐渐地演变，各设备的位置可灵活调整和改变。

③ 提高了系统的可靠性、可用性。

局域网的应用范围极广，可应用于办公自动化、生产自动化、企事业单位的管理、银行业务处理、军事指挥控制、商业管理等方面。局域网的主要功能是为了实现资源共享，其次是为了更好地实现数据通信与交换，以及数据的分布处理。

### 4.1.2　常见的局域网拓扑结构

拓扑这个名词是从几何学中借用来的，网络拓扑是网络形状，或者是它在物理上的连通性。在计算机网络中，把计算机、终端、通信处理机等设备抽象成点，把连接这些设备的通信线路抽象成线，并将由这些点和线所构成的拓扑称为网络拓扑结构。网络拓扑结构反映出网络的结构关系，它对于网络的性能、可靠性以及建设管理成本等都有着重要的影响，主要有星形结构、环形结构、总线形结构、分布式结构、树形结构、网状结构、蜂窝状结构等。

#### 1．星形拓扑（Star-Topology）

星形拓扑是由中央节点和通过点对点链路接到中央节点的各站点（网络工作站等）组成，如图 4.1 所示。星形拓扑以中央节点为中心，执行集中式通信控制策略，因此，中央节点相当复杂，而各个站的通信处理负担都很小，又称集中式网络。中央控制器是一个具有信号分离功能的“隔离”装置，它能放大和改善网络信号，外部有一定数量的端口，每个端口连接一个站点，如 Hub 集线器、交换机等。采用星形拓扑的交换方式有线路交换和报文交换，尤以线路交换更为普遍，现有的数据处理和声音通信的信息网大多采用这种拓扑。一旦建立了通信的连接，可以没有延迟地在两个连通的站点之间传输数据。

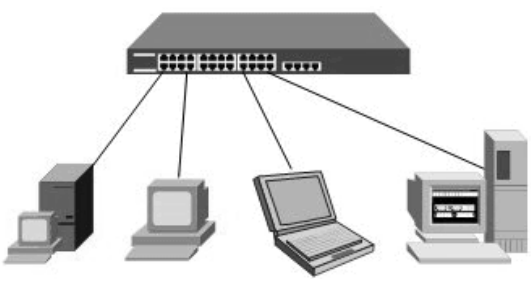


图 4-1　星形拓扑结构

星形拓扑的优点是结构简单、管理方便、可扩充性强、组网容易。利用中央节点可方便地提供网络连接和重新配置；且单个连接点的故障只影响一个设备，不会影响全网，容易检测和隔离故障，便于维护。

星形拓扑的缺点是每个站点直接与中央节点相连，需要大量电缆，因此费用较高；如果中央节点产生故障，则全网不能工作，所以对中央节点的可靠性和冗余度要求很高。星形拓扑广泛应用于网络中智能集中于中央节点的场合。

### 2．总线形拓扑（Bus Topology）

总线形拓扑采用单根传输线作为传输介质，所有的站点都通过相应的硬件接口直接连接到传输介质或总线上。任何一个站点发送的信息都可以沿着介质传播，而且能被所有其他的站点接收。如图 4-2 所示的是总线形拓扑，如图 4-3 所示的是带有中继器的总线形拓扑。

图 4-2　典型的总线形拓扑结构

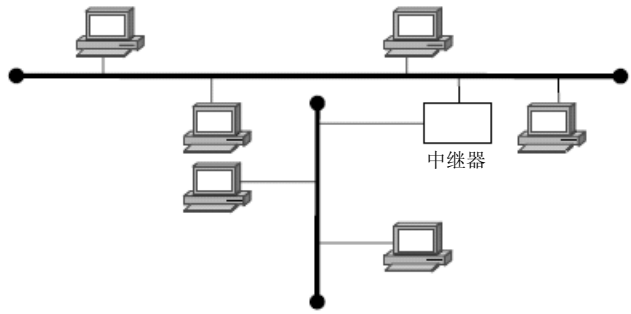



图 4-3　带有中继器的总线形拓扑

由于所有的站点共享一条公用的传输链路，所以一次只能有一个设备传输数据。通常采用分布式控制策略来决定下一次哪一个站点发送信息。发送时，发送站点将报文分组，然后一次一次地依次发送这些分组，有时要与其他站点发来的分组交替地在介质上传输。当分组经过各站点时，目的站点将识别分组中携带的目的地址，然后复制这些分组的内容。这种拓扑减轻了网络通信处理的负担，它仅仅是一个无源的传输介质，而通信处理分布在各站点进行。总线拓扑的优点是结构简单、实现容易；易于安装和维护；价格低廉，用户站点入网灵活。总线形拓扑结构的缺点是传输介质故障难以排除，并且由于所有节点都直接连接在总线上，因此任何一处故障都会导致整个网络的瘫痪。不过，对于站点不多（10 个站点以下）的网络或各个站点相距不是很远的网络，采用总线拓扑还是比较适合的。但随着在局域网上传输多媒体信息的增多，目前这种网络正在被淘汰。

### 3．环形拓扑（Ring Topology）

环形拓扑由一些中继器和连接中继器的点到点链路首尾相连形成一个闭合的环。如图 4-4 所示，每个中继器都与两条链路相连，它接收一条链路上的数据，并以同样的速度串行地把

该数据送到另一条链路上，而不在中继器中缓冲。这种链路是单向的，也就是说，只能在一个方向上传输数据，而且所有的链路都按同一方向传输，数据就在一个方向上围绕着环进行循环。

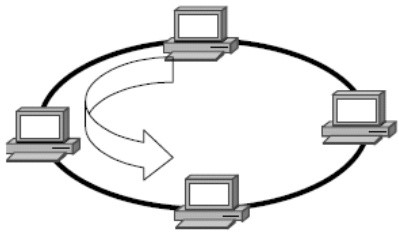


图 4-4　环形拓扑结构

由于多个设备共享一个环，因此需要对此进行控制，以便决定每个站在什么时候可以把分组放在环上。这种功能是用分布控制的形式完成的，每个站都有控制发送和接收的访问逻辑。由于信息包在封闭环中必须沿每个节点单向传输，因此，环中任何一段的故障都会使各站之间的通信受阻。为了增加环形拓扑的可靠性，还引入了双环拓扑。所谓双环拓扑就是在单环的基础上在各站点之间再连接一个备用环，从而当主环发生故障时，由备用环继续工作。环形拓扑结构的优点是能够较有效地避免冲突，其缺点是环形结构中的网卡等通信部件比较昂贵且管理复杂得多。在实际的应用中，多采用环形拓扑作为宽带高速网络的结构。

### 4．树形拓扑（Tree Topology）

树形拓扑是从总线拓扑演变而来的，它把星形和总线形结合起来，形状像一棵倒置的树，顶端有一个带分支的根，每个分支还可以延伸出子分支，如图 4-5 所示。

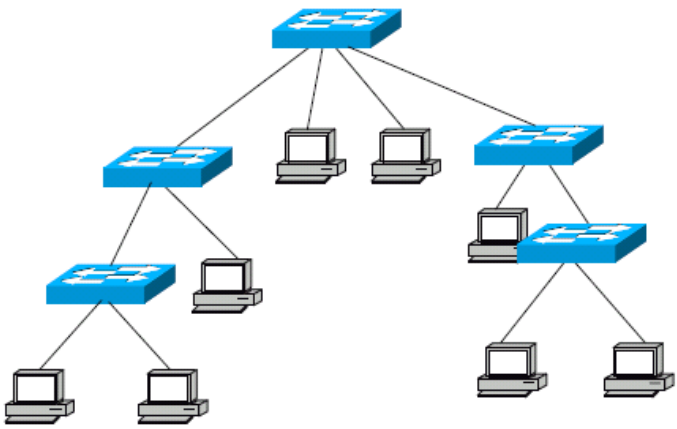


图 4-5　树形网络拓扑结构

这种拓扑和带有几个段的总线拓扑的主要区别在于根的存在。当节点发送时，根接收该信号，然后再重新广播发送到全网。

树形拓扑的优点是易于扩展和故障隔离，树形拓扑的缺点是对根的依赖性太大，如果根发生故障，则全网不能正常工作，对根的可靠性要求很高。

### 5．星形环拓扑

星形环拓扑是将星形拓扑和环形拓扑混合起来的一种拓扑，试图取这两种拓扑的优点于一个系统中，克服了典型的星形和典型的环形两个拓扑的不足和缺陷。这种拓扑的配置是由一批接在环上的连接集中器（实际上是指安装在楼内各层的配线架）组成，从每个集中器按星形结构接至每个用户站上，如图 4-6 所示。

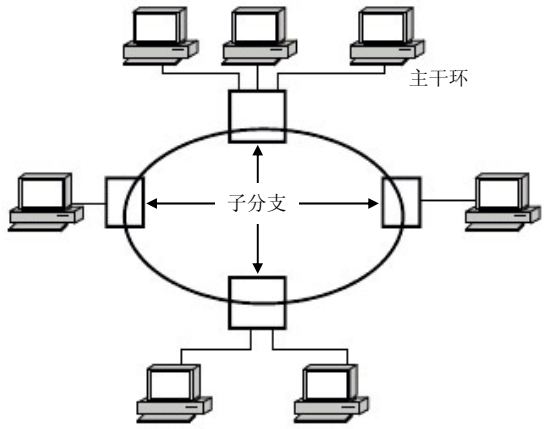



图 4-6　星形环拓扑

星形环拓扑的优点是故障诊断和隔离、易于扩展、安装电缆方便。星形环拓扑的缺点是需要智能的集中器、电缆安装电缆长、安装不方便等。

**6．拓扑的选择**

拓扑的选择往往和传输介质的选择，以及介质访问控制方法的确定紧密相关。选择拓扑时，应该考虑的主要因素有以下几点。

（1）经济性

网络拓扑的选择直接决定了网络安装和维护的费用。不管选用什么样的传输介质，都需要进行安装。例如，安装电线沟、安装电线管道等。最理想的情况是建楼以前先进行安装，并考虑今后扩建的要求。安装费用的高低与拓扑结构的选择以及传输介质的选择、传输距离的确定有关。

（2）灵活性

灵活性以及可扩充性也是选择网络拓扑结构时应充分重视的问题。任何一个网络，随着用户数的增加，网络应用的深入和扩大，网络新技术的不断涌现，特别是应用方式和要求的改变，网络经常需要加以调整。网络的可调整性与灵活性以及可扩充性都与网络拓扑直接相关。一般说来，总线形拓扑和环形拓扑要比星形拓扑的可扩充性好得多。

（3）可靠性

网络的可靠性是任何一个网络的生命。网络拓扑决定了网络故障检测和故障隔离的方便性。总之，选择局域网拓扑时，需要考虑的因素很多，这些因素同时影响网络的运行速度和网络软/硬件接口的复杂程度等。

## 4.1.3　局域网的体系结构

从本质上说，局域网是一个通信网，其协议应该包括 OSI 协议的低三层，即物理层、数据链路层和网络层，但由于局域网的网络结构比较简单，在 LAN 中也就没有路由问题，任何两点之间可用一条直接的链路，所以，也不需要单独设置网络层，而可将寻址、排序、流控和差错控制等功能放在数据链路层中去实现。

下面详细介绍局域网参考模型与 OSI 参考模型的关系，如图 4-7 所示。局域网的参考模型只对应于 OSI 参考模型的数据链路层与物理层，它将数据链路层划分为两个子层：逻辑链路控制（Logical Link Control，LLC）子层与介质访问控制（Media Access Control，MAC）子层。

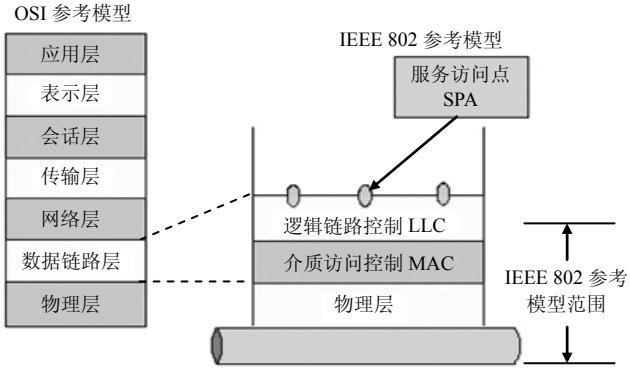



图 4-7　局域网参考模型与 OSI 参考模型的关系

### 1．物理层

物理层涉及通信时在信道上传输的原始比特流，它的主要作用是确保在一段物理链路上二进制比特信号的正确传输。物理层的主要功能包括信号的编码/解码、同步前导码的生成与去除、二进制比特信号的发送与接收。另外，为确保位流的正确传输，物理层还具有错误校验功能，以保证比特信息的正确发送与接收。这就是说物理层必须保证在双方通信时，一方发送二进制“1”；另一方接收的也是“1”。

局域网物理层制定的标准规范的主要内容如下。

（1）局域网所支持的传输介质与传输距离；

（2）传输速率；

（3）物理接口的机械特性、电气特性、性能特性和规程特性；

（4）传输信号的编码方案，局域网常用的编码方案有：曼彻斯特编码、差分曼彻斯特编码、4B/5B 和 8B/10B 等编码；

（5）差错校验码及同步信号的产生与删除；

（6）拓扑结构。

### 2．MAC 子层

介质访问控制子层（MAC）是数据链路层的一个功能子层，MAC 子层构成了数据链路层的下半部，它直接与物理层相邻，主要负责制定管理和分配信道的协议规范。

MAC 子层的主要功能是进行合理的信道分配，解决信道竞争问题。它在数据链路层中，完成介质访问控制功能，为竞争用户分配信道的使用权，并具有管理多链路的功能。MAC 子层为不同的物理介质定义了介质访问控制标准。目前，IEEE 802 已制定的介质访问控制标准有著名的带有冲突检测功能的载波监听多路访问（CSMA/CD）、令牌环（Token Ring）和令牌总线（Token BUS）等。介质访问控制方法决定了局域网的主要性能，它对局域网的响应时间、吞吐量和带宽利用率等性能都有十分重大的影响。

MAC 子层的另一个主要功能是在发送数据时，将从上层接收的数据（PDU-LLC 协议数据单元）组装成带 MAC 地址和差错检测字段的数据帧；在接收数据时拆帧，并完成地址识别和差错检测。

### 3．LLC 子层

逻辑链路控制子层（LLC）也是数据链路层的一个功能子层。它构成了数据链路层的上半部分，与网络层和 MAC 子层相邻。LLC 子层在 MAC 子层的支持下向网络层提供服务。它可运行于所有 802 局域网和城域网的协议之上。LLC 子层与传输介质无关，它独立于介质访问控制方法，隐藏了各种局域网技术之间的差异，向网络层提供一个统一的格式与接口。

LLC 子层的作用是在 MAC 子层提供的介质访问控制和物理层提供的比特服务的基础上，将不可靠的物理信道处理为单一的、可靠的逻辑信道，确保数据帧的正确传输。

LLC 子层的主要功能是建立、维持和释放数据链路，提供一个或多个服务访问点，为网络层提供面向连接和无连接服务。另外，为保证通过局域网的无差错传输，LLC 子层还提供差错控制和流量控制，以及发送顺序控制等功能。

## 4.1.4 IEEE 802 标准

1980 年 2 月成立了局域网标准化委员会，即 IEEE 802 委员会（Institute of Electrical and Electronics Engineers INC，IEEE，电器和电子工程师协会）。该委员会制定了一系列局域网标准，称为 IEEE 802 标准。该标准已被国际标准化组织 ISO 采纳，作为局域网的国际标准。IEEE 802 的体系结构如图 4-8 所示。

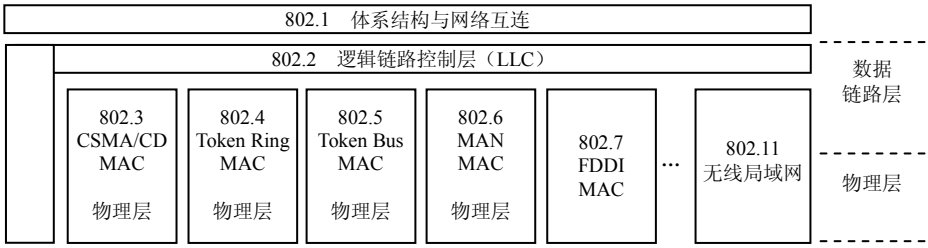



图 4-8 IEEE 802 的体系结构

目前，IEEE 802 系列标准主要有以下几种：

IEEE 802.1：局域网概述、体系结构、网络管理和网络互连。

IEEE 802.2：定义逻辑链路控制（LLC）。

IEEE 802.3：定义 CSMA/CD 媒体访问控制方法和物理层规范。

IEEE 802.4：令牌总线（Token Passing Bus）。

IEEE 802.5：令牌环（Token Ring）访问方法和物理层规范。

IEEE 802.6：城域网访问方法和物理层规范。

IEEE 802.7：宽带技术。

IEEE 802.8：光纤技术。

IEEE 802.9：综合声音/数据服务的访问方法和物理规范。

IEEE 802.10：安全与加密访问方法和物理层规范。

IEEE 802.11：无线局域网访问方法和物理层规范，包括 IEEE 802.11a、IEEE 802.11b、IEEE 802.11c 和 IEEE 802.11q 标准。

IEEE 802.12：100VG-AnyLAN 快速局域网访问方法和物理层规范。

## 4.2　介质访问控制方法

将传输介质的频带有效地分配给网上各站点用户的方法称为介质访问控制方法。介质访问控制方法是局域网最重要的一项基本技术，对局域网体系结构、工作过程和网络性能产生决定性影响。设计一个好的介质访问控制协议有三个基本目标：协议要简单，获得有效的通道利用率，公平合理地对待网上各站点的用户。介质访问控制方法主要是解决介质使用权的算法或机构问题，从而实现对网络传输信道的合理分配。

### 4.2.1　信道分配问题

通常，可将信道分配方法划分为两类：静态分配方法和动态分配方法。

#### 1．静态分配方法

所谓静态分配方法，也是传统的分配方法，它采用频分多路复用或时分多路复用的方法将单个信道划分后静态地分配给多个用户。当用户站数较多或使用信道的站数在不断变化或者通信量的变化具有突发性时，静态频分多路复用方法的性能较差，因此，传统的静态分配方法，不完全适合计算机网络。

#### 2．动态分配方法

所谓动态分配方法就是动态地为每个用户站点分配信道使用权。动态分配方法通常有三种：轮转、预约和争用。

① 轮转：使每个用户站点轮流获得发送的机会，这种技术称为轮转。它适合于交互式终端对主机的通信。

② 预约：预约是指将传输介质上的时间分隔成时间片，网上用户站点若要发送，必须事先预约能占用的时间片。这种技术适用于数据流的通信。

③ 争用：若所有用户站点都能争用介质，这种技术称为争用。它实现起来简单，对轻负载或中等负载的系统比较有效，适合于突发式通信。争用方法属于随机访问技术，而轮转和预约的方法则属于控制访问技术。

### 4.2.2　介质访问控制方法

介质访问控制方法的主要内容有两个方面：一是要确定网络上每一个节点能够将信息发送到介质上去的特定时刻；二是要解决如何对共享介质访问和利用加以控制。常用的介质访

问控制方法有三种：总线形结构的带冲突检测的载波监听多路访问 CSMA/CD 方法、环形结构的令牌环（Token Ring）访问控制方法和令牌总线（Token Bus）访问控制方法。

### 1．总线形结构的带冲突检测的载波监听多路访问 CSMA/CD 方法

CSMA/CD（Carrier Sense Multiple Access/Collision Detection）是采用争用技术的一种介质访问控制方法。CSMA/CD 通常用于总线形拓扑结构和星形拓扑结构的局域网中。它的每个站点都能独立决定发送帧，若两个或多个站同时发送，即产生冲突。每个站都能判断是否有冲突发生，如冲突发生，则等待随机时间间隔后重发，以避免再次发生冲突。CSMA/CD 的工作原理可概括成四句话，即先听后发、边发边听、冲突停止、随机延迟后重发。具体过程如下：

① 当一个站点想要发送数据时，它检测网络查看是否有其他站点正在传输，即监听信道是否空闲。

② 如果信道忙，则等待，直到信道空闲。

③ 如果信道闲，站点就传输数据。

④ 在发送数据的同时，站点继续监听网络确信没有其他站点在同时传输数据。因为有可能两个或多个站点都同时检测到网络空闲然后几乎在同一时刻开始传输数据。如果两个或多个站点同时发送数据，就会产生冲突。

⑤ 当一个传输节点识别出一个冲突时，它就会发送一个拥塞信号，这个信号使得冲突的时间足够长，让其他的节点都能发现。

⑥ 其他节点收到拥塞信号后，都停止传输，等待一个随机产生的时间间隙（回退时间，Backoff Time）后重发。

总之，CSMA/CD 采用的是一种“有空就发”的竞争型访问策略，因而不可避免地会出现信道空闲时多个站点同时争发的现象，无法完全消除冲突，只能是采取一些措施减少冲突，并对产生的冲突进行处理。因此采用这种协议的局域网环境不适合对实时性要求较强的网络应用。

### 2．令牌环（Token Ring）访问控制

Token Ring 是令牌传输环（Token Passing Ring）的简写。令牌环介质访问控制方法，是通过在环形网上传输令牌的方式来实现对介质的访问控制。只有当令牌传输至环中某站点时，它才能利用环路发送或接收信息。当环线上各站点都没有帧发送时，令牌标记为 01111111，称为空标记。当一个站点要发送帧时，需等待令牌通过，并将空标记置换为忙标记 01111110，紧跟着令牌，用户站点把数据帧发送至环上。由于是忙标记，所以其他站点不能发送帧，必须等待。

发送出去的帧将随令牌沿环路传输下去。在循环一周又回到原发送站点时，由发送站点将该帧从环上移去，同时将忙标记换为空标记，令牌传至后面站点，使之获得发送的许可权。发送站点在从环中移去数据帧的同时还要检查接收站载入该帧的应答信息，若为肯定应答，说明发送的帧已被正确接收，完成发送任务。若为否定应答，说明对方未能正确收到所发送的帧，原发送站点需在带空标记的令牌第二次到来时，重发此帧。采用发送站从环上收回帧的策略，不仅具有对发送站点自动应答的功能，而且还具有广播特性，即可有多个站点接收同一数据帧。接收帧的过程与发送帧不同，当令牌及数据帧通过环上站点时，该站将帧携带的目标地址与本站地址相比较。若地址符合，则将该帧复制下来放入接收缓冲器中，待接收

站正确接收后，即在该帧上载入肯定应答信号；若不能正确接收则载入否定应答信号，之后再将该帧送入环上，让其继续向下传输。若地址不符合，则简单地将数据帧重新送入环中。所以当令牌经过某站点而它既不发送信息，又无处接收时，会稍经延迟，继续向前传输。在系统负载较轻时，由于站点需等待令牌到达才能发送或接收数据，因此效率不高。但若系统负载较重，则各站点可公平共享介质，效率较高。为避免所传输数据与标记形式相同而造成混淆，可采用位填入技术，以区别数据和标记。使用令牌环介质访问控制方法的网络，需要有维护数据帧和令牌的功能。如可能会出现因数据帧未被正确移去而始终在环上传输的情况。也可能出现令牌丢失或只允许一个令牌的网络中出现了多个令牌等异常情况。解决这类问题的办法是在环中设置监控□ 85 □器，对异常情况进行检测并消除。令牌环网上的各个站点可以设置成不同的优先级，允许具有较高优先权的站申请获得下一个令牌权。

归纳起来，在令牌环中主要有以下三种操作：

① 截获令牌并且发送数据帧。如果没有节点需要发送数据，令牌就由各个节点沿固定的顺序逐个传递；如果某个节点需要发送数据，它要等待令牌的到来，当空闲令牌传到这个节点时，该节点修改令牌帧中的标志，使其变为“忙”的状态，然后去掉令牌的尾部，加上数据，成为数据帧，并发送到下一个节点。

② 接收与转发数据。数据帧每经过一个节点，该节点就比较数据帧中的目的地址，如果不属于本节点，则转发出去；如果属于本节点，则复制到本节点的计算机中，同时在帧中设置已经复制的标志，然后向下一节点转发。

③ 取消数据帧并且重发令牌。由于环网在物理上是个闭环，一个帧可能在环中不停地流动，所以必须清除。当数据帧通过闭环重新传到发送节点时，发送节点不再转发，而是检查发送是否成功。如果发现数据帧没有被复制（传输失败），则重发该数据帧；如果发现传输成功，则清除该数据帧，并且产生一个新的空闲令牌发送到环上。

#### 3．令牌总线（Token Bus）访问控制

令牌总线访问控制是在物理总线上建立一个逻辑环，令牌在逻辑环路中依次传递，其操作原理与令牌环相同。它同时具有上述两种方法的优点，是一种简单、公平、性能良好的介质访问控制方法。

## 4.3　局域网的组成

局域网由网络硬件和网络软件两大部分组成。网络硬件用于实现局域网的物理连接，为连接在局域网上的各计算机之间的通信提供一条物理通道。网络软件用来控制并具体实现通信双方的信息传递和网络资源的分配与共享。

### 4.3.1　局域网的硬件系统

网络硬件主要由计算机系统和通信系统组成。计算机系统是局域网的连接对象，是网络的基本单元。它具有访问网络资源、管理和分配网络共享资源及数据处理的能力。根据计算

机系统提供的功能和在网络中的作用，联网计算机可分为网络服务器和网络工作站两种类型。

通信系统是连接网络基本单元的硬件系统，主要作用是通过传输介质（传输媒体）和网络设备等硬件系统将计算机连接在一起，为它们提供通信功能。

通信系统主要包括：

（1）网络设备（如 Hub、交换机、路由器等）。

（2）网络接口卡（如网卡、粗缆收发器、光纤收发器等）。

（3）传输介质（如同轴电缆、双绞线、光纤等）及其介质连接部件（如水晶头、T 形接头等）。

总体上讲，局域网硬件应包括：网络服务器、网络工作站、网络接口卡、网络设备、传输介质及介质连接部件，以及各种适配器等。

当建立一个局域网时，必须在每台联网计算机上安装网络接口卡，然后通过传输介质和介质连接部件，将计算机连接起来或将计算机与网络设备连接起来以实现局域网的物理连接。根据不同的联网技术，需要使用的网络设备不尽相同。例如：采用 100Mbps 交换式以太网技术组建一个局域网，其硬件设备包括计算机系统、100Mbps 网络接口卡（网卡）、快速以太网交换机（Switch）、非屏蔽双绞线（UTP）及 RJ-45 标准接口部件。

下面将逐个介绍网络服务器、网络工作站、网络接口卡、网络设备、传输介质及其介质连接部件的功能与应用。

### 1．网络服务器

网络服务器是连接在局域网上的一台计算机，称为网络节点。该节点的特殊功能是为网络用户提供各种网络服务和共享资源。这种为网络用户提供服务和共享资源的网络节点就称为网络服务器。网络服务器是局域网的核心，它拥有大量可共享的硬件资源（如大容量的磁盘和高速打印机、高性能绘图仪等贵重的外围设备）和软件资源（如数据库、信息、文件系统、应用软件等），并具有管理这些资源和协调网络用户访问资源的能力。

### 2．网络工作站

网络工作站是指用户能够在网络环境中工作，访问网络共享资源的计算机系统，通常又称为客户机（Client）。

网络工作站是连接在局域网上的一台计算机，用户通过它来访问网络，共享资源。它的主要作用是为网络用户提供一个访问网络服务器，共享网络资源，与网上其他节点交流信息的操作台和前端窗口，使用户能够在网上工作，如网上传输文件、共享打印机打印文件、访问 Internet 上的各种信息服务和共享网上的各种软/硬件资源等。

在网络工作站上，必须安装一块网络接口卡，并通过传输介质及介质连接设备和网络设备把它连接到网络上，成为局域网上的一个工作站点。在网络工作站上，除运行自己的操作系统（如 DOS、PS/2．Windows、UNIX 等）外，还必须运行有关的网络软件，包括：网络协议软件（如 TCP/IP、IPX 协议软件）、网络应用软件（如 Internet 各种信息服务的客户软件）或网络操作系统的客户端软件（如 NetWare 外壳软件）。用户在网络工作站上，使用网络软件提供的实用程序或操作命令向服务器申请网络服务，获取各种公共的网络资源，访问 Internet 信息服务等。网络工作站不仅能够访问本机的本地资源，同时也能访问网络上所有的远程资源（只要权限允许）。当网络工作站不在网上操作时，仍可作为一台独立的计算机使用。

### 3．网络接口卡

网络接口卡（Network Interface Card，NIC），又称为网络适配器（Network Interface Adapter，NIA），简称网卡，网卡是安装在计算机中的一块电路板，它可以作为计算机的外部设备插在扩展槽中，用于实现计算机和传输介质之间的物理连接，为计算机之间相互通信提供一条物理通道，并通过这条通道进行高速数据传输。在局域网中，每一台联网计算机都需要安装一块或多块网卡，通过介质连接器件将计算机接入网络电缆系统。

网卡工作在数据链路层，它主要完成物理层和数据链路层中 MAC 子层的功能，如网卡与传输介质的连接、介质访问控制（如 CSMA/CD）的实现、数据帧的拆装、帧的发送与接收、错误校验、数据信号的编/解码（如曼彻斯特代码的转换）、数据的串－并转换及网卡与计算机之间的数据交换等。网卡是局域网通信接口的关键设备，它是决定计算机网络性能指标的重要因素之一。

网卡最基本的功能包括：数据转换、通信服务和数据缓存。

每一块网卡上都存储有一个物理地址，称为 MAC 地址，符合 IEEE 标准的网卡具有唯一的 MAC 地址。他是一个被固化在 ROM 中的 6 字节的二进制数据，通常按字节以十六进制的形式表示，如 FA-32-56-CD-24-1C，其中前 3 个字节是生产厂家的编号，后 3 个字节为该厂家的产品序号。

网卡工作时需要一个网卡驱动程序，它被装配在网卡所在的主机上。网卡驱动程序是运行在 OSI 参考模型的数据链路层上的软件，完成 MAC 子层的功能。

网卡可按接头、总线接口（BUS）以及带宽（Bandwidth）3 种方式进行分类。按接头分类有：AUI 接头、BNC 接头、RJ-45 接头、RJ-45+BNC 双口网卡等。按总线接口划分有：ISA 接口、PCI 接口、USB 接口和 PCMCIA 接口。

PCMCIA 网卡是用于笔记本电脑的一种网卡，大小与扑克牌差不多，PCMCIA 总线分为两类，一类为 16 位的 PCMCIA，另一类为 32 位的 CardBus。

USB 作为一种新型的总线技术，由于传输速率远远大于传统的并行口和串行口，设备安装简单又支持热插拔，已被广泛应用于鼠标、键盘、打印机、扫描仪、MODEM、音箱等各类设备中，网络适配器自然也不例外。USB 网络适配器其实是一种外置式网卡。

按照传输速率的不同，网卡可以分为 10Mbps、100Mbps、1 000Mbps、10Mbps/100Mbps 自适应网卡等几类。

按网卡支持的网络协议分类有以太网卡、快速以太网卡、千兆以太网卡、FDDI 网卡、ATM 网卡等。常见的网卡类型如图 4-9 所示。

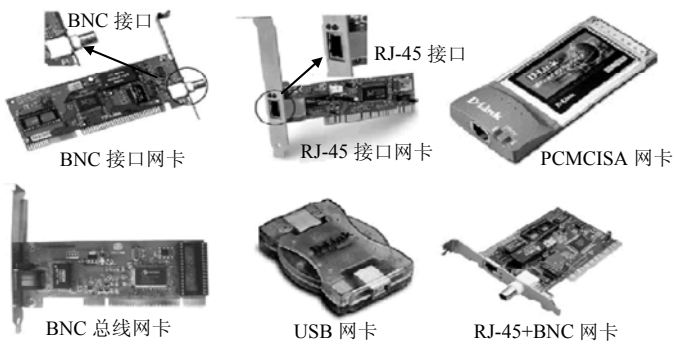



图 4-9　常见的网卡类型

选用什么类型的网卡，需要根据实际的网络环境而定，具体来说网卡的选型需根据所使用的局域网标准、传输介质和计算机的总线类型来选择。

#### 4．网络设备

这里的网络设备是指单个计算机连入网络及网络与网络互连时必须使用的设备。是集线器（HUB）、中继器（Repeater）、交换机（Switch）等网络连接设备和网桥（Bridge）、路由器（Router）、网关等网络互连设备的统称。通过这些设备可以把计算机连接起来组成局域网，或将局域网与局域网互连起来组成更大规模的互联网。网络设备是组建计算机网络的关键部件。比如：将计算机通过以太网卡、非屏蔽双绞线、RJ-45 连接器和网络交换机相连，就能组成一个 10Base-T 以太网，如图 4-10 所示。

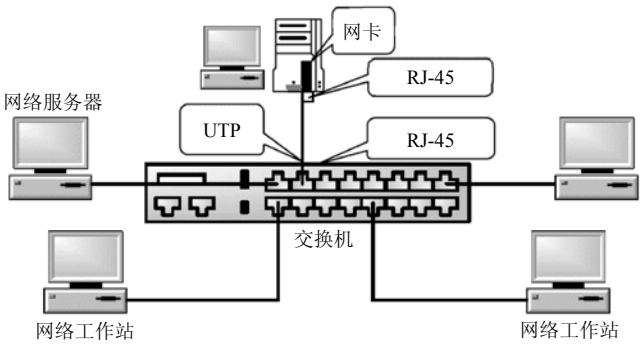



图 4-10　10Base-T 以太网

#### 5．传输介质

传输介质是通信双方交流信息的物理通道，用于两个网络站点之间原始比特流的实际传输。传输介质的品种繁多，每一种介质在带宽、延迟、信号衰减、抗干扰能力、传输距离、安装维护难度等方面都不相同。传输介质的选用是非常重要的，它对网络性能影响极大。在局域网中，常用的是有线传输介质，主要有非屏蔽双绞线、屏蔽双绞线、同轴电缆和光纤。

### 4.3.2　网络软件

网络软件是一种在网络环境下运行和使用，或者说控制与管理网络运行的软件，是一种使通信双方能够交流信息的软件。根据网络软件的功能与作用，可分为网络系统软件和网络应用软件。

#### 1．网络系统软件

网络系统软件是控制和管理网络运行、提供网络通信和网络资源分配与共享功能的网络软件，它为用户提供了访问网络和操作网络的友好界面。网络系统软件主要包括网络操作系统（NOS）、网络协议软件和网络通信软件等。常用的网络操作系统有 Windows NT、Windows Server 2003、UNIX 和 Netware，常用的网络协议软件有 TCP/IP 和 SPX/IPX，常用的通信软件有各种类型的网卡驱动程序等。

### 2．网络应用软件

网络应用软件是指为某一个应用目的而开发的网络软件，它为用户提供一些实际的应用，网络应用软件既可用于管理和维护网络本身，也可用于某一个业务领域。常用的网络应用软件有网络管理监控程序、网络安全软件、分布式数据库、管理信息系统（MIS）、数字图书馆、Internet 信息服务、远程教学、远程医疗、视频点播等。网络应用的领域极为广泛，应用软件也极为丰富。现在人们越来越认识到网络应用的重要性，各界人士都在关注着网络应用软件的开发。

## 4.4　局域网的工作模式

### 4.4.1　对等结构网络

对等结构网络也叫工作组网，是把联网计算机组成一个工作组，且联入网内的计算机具有平等的地位，网络中没有服务器，用户只能简单的通过网络，在独立的同级系统间共享资源。

#### 1．对等网的特点

对等网组建方式简单，投资成本低，非常适合家庭及小型企业用户使用。它具有如下几方面的基本特点：

（1）网络用户较少，一般在 20 台以内比较适宜。

（2）网络用户都处于同一区域内，地位平等，无主次之分。

（3）网络用户既可以作为服务器提供网络资源，又可以以工作站方式享用资源。

（4）共享资源分散存放在各个工作站上。

（5）缺乏统一的身份认证机制，数据保密性差，网络安全性差。

#### 2．对等网的硬件连接

对等网的连接比较简单，当计算机互连时，只需使用交叉线互连两台计算机的网卡即可。在多台计算机互连时，需购买一台交换机或集线器，使用直通线连接交换机和主机网卡，即可组成一个星形结构的网络。

#### 3．协议配置

在 Windows 系统中，只要正确安装了网络适配器，就会自动安装 TCP/IP 协议，并可设置 IP 地址信息。设置方法如下：

（1）在控制面板中双击“网络和 Internet 连接”，再双击“本地连接”并单击“属性”按钮，打开“本地连接属性”对话框，然后选择 TCP/IP 协议并单击“属性”按钮，即可出现如图 4-11 所示的对话框。

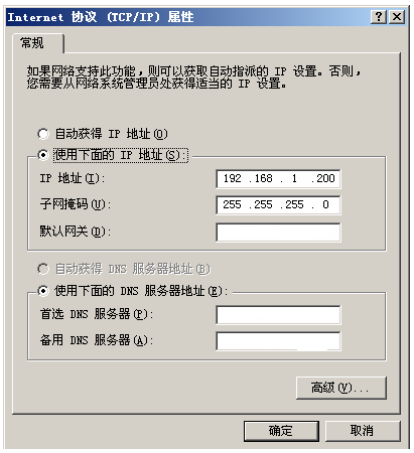



图 4-11　IP 配置

（2）选择“使用下面的 IP 地址”单选按钮，然后设

置 IP 地址、子网掩码等信息。

（3）单击“确定”按钮退出设置界面。

### 4．文件共享

（1）打开“控制面板”，双击“网络连接”，然后选择“设置或更改您的家庭或小型办公网络”连接，即可运行网络安装向导，如图 4-12 所示。

（2）连续单击“下一步”按钮，在图 4-13 的“选择连接方法”对话框中，选中“其他”单选按钮。


图 4-12　运行网络安装向导

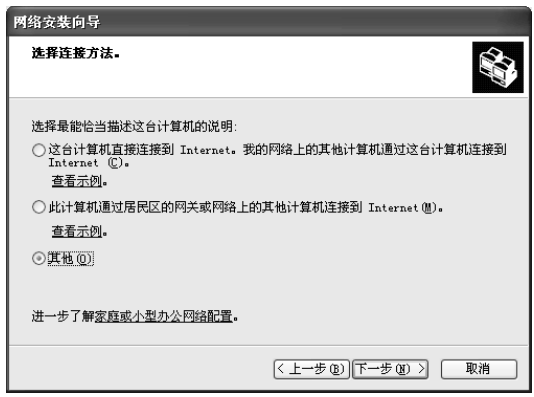



图 4-13　选择连接方法

（3）单击“下一步”按钮，在打开的“其他 Internet 连接方法”对话框中，选中“这台计算机属于一个没有 Internet 连接的网络”单选按钮，如图 4-14 所示。

（4）然后单击“下一步”按钮，完成后面的“计算机描述”、“计算机名”、“工作组”等设置，如图 4-15 和图 4-16 所示。


图 4-14　“其他 Internet 连接方法...”对话框


图 4-15　计算机名描述

（5）在设置完工作组名后，打开“文件和打印机共享”对话框，选中“启用文件和打印机共享”单选按钮，如图 4-17 所示。

（6）单击“下一步”按钮，在弹出的对话框中单击“确定”按钮，即可开始配置网络。配置完成后，弹出如图 4-18 所示对话框，选择合适的选项。

（7）单击“下一步”按钮，并在打开的对话框中单击“完成”按钮，完成家庭及小型办

公室网络的配置，如图 4-19 所示。

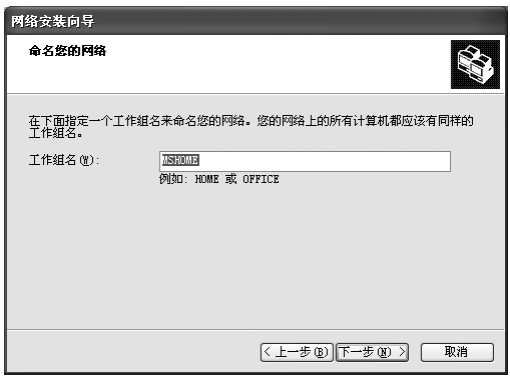



图 4-16　工作组设置


图 4-17　启用文件和打印机共享

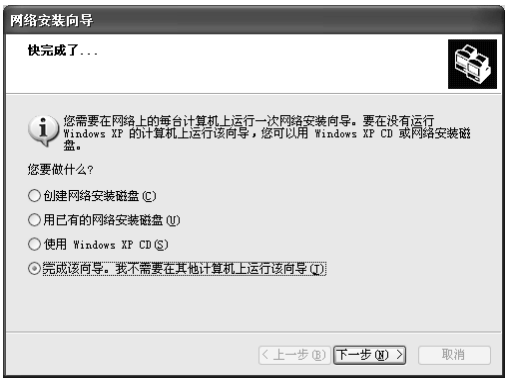



图 4-18　其他选项设置

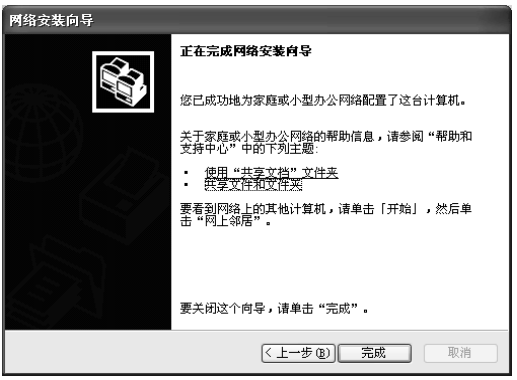



图 4-19　完成向导

（8）右击需共享的文件夹，在弹出的快捷菜单中选择“属性”命令，打开“共享文档属性”对话框，选择“共享”选项卡，如图 4-20 所示。

选择“共享此文件夹”选项，然后单击“权限”按钮，打开如图 4-21 所示的对话框。可根据需要设置用户权限为：“完全控制”、“读取”或“更改”。


图 4-20　共享选项卡


图 4-21　用户权限设置

若安装了 Windows XP，系统将自动启用 Windows 防火墙。防火墙将禁止其他用户访问共享文件夹。若实现共享文件夹的发布，应在控制面板中将防火墙关闭。

### 5．打印机共享

（1）通过选择“开始”→“设置”→“打印机和传真”命令，打开“打印机和传真”管理窗口，如图 4-22 所示。

（2）在列表框内选择需要共享的打印机图标，右击该图标，打开快捷式菜单，选中执行“共享”命令，如图 4-23 所示。


图 4-22　打印机和传真


图 4-23　设置共享

（3）在弹出的“打印机属性”对话框内，选择“共享”选项卡，并选中“共享这台打印机”选项，输入共享名称，然后单击“应用”、“确定”按钮，完成共享设置，如图 4-24 所示。

（4）完成共享后，打印机和传真管理窗口里的相应打印机图标上会多出手形的共享标记，表示共享设置成功，如图 4-25 所示。


图 4-24　共享选项设置


图 4-25　设置完成后的共享

## 4.4.2　客户机/服务器模式

由于处理器技术、计算机技术和网络技术的进一步发展，使得计算机的处理能力更加增

强，而路由器和网桥技术的应用和有效地网络管理使得计算机连接到局域网上变得更加容易，通过各种网络新技术可以将地理上分散的局域网互联在一起。联网计算机可以很方便地访问大型系统的各种信息。另外，个人计算机的价格不断下降也使得个人计算机的使用日益广泛。

正是基于以上原因，人们已经不满足于资源共享模式，而是开发出一种新的信息组织模式，这就是客户机/服务器模式，简称 C/S 模式，其网络结构如图 4-26 所示。

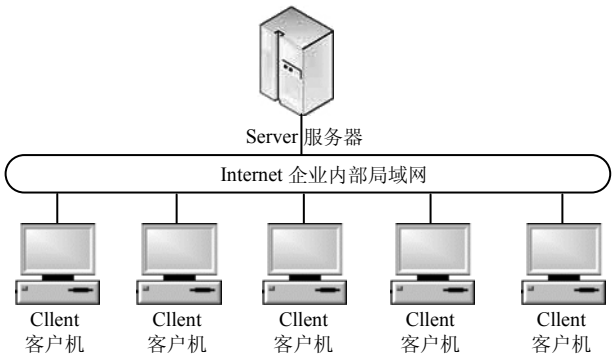



图 4-26　C/S 网络模式

在客户机/服务器模式下，一个或更多个客户机和一个或更多的服务器，以及支持客户机和服务器进程通信的网络操作系统，共同组成了一个支持分布计算、分析和表示的系统；在 C/S 模式中，客户方发出请求，网络通信系统将请求的内容传送到服务器，服务器根据请求完成预定的操作，然后把结果送回客户。

C/S 模式的主要特点：

（1）属于二层结构的资源共享模式，可用于共享应用、数据和打印机等服务；

（2）所有的用户查询或命令处理都在工作站上完成；

（3）利用工作站的能力运行所有应用，利用服务器的能力来作为外设的延伸，如硬盘、打印机等；

（4）应用被分为前端（客户端）和后端（服务器端）。

在 C/S 模式中，客户机和服务器分别工作在不同的逻辑实体中，并协同工作。服务器主要是运行客户机不能完成或费时的工作，如大型数据库的管理；而客户机可以通过预先指定的语言向服务器提出请求，要求服务器去执行某项操作，并将操作结果返送给客户机。

### 4.4.3　浏览器/服务器模式

随着 Internet/Intranet 技术和应用的发展，一种新的网络信息组织模式在 20 世纪 90 年代中期逐渐形成和发展，这种基于浏览器、WWW 服务器和应用服务器的计算结构称为浏览器/服务器 （Browser/Server）的计算模式，简称 B/S 模式，其网络结构如图 4-27 所示。

在 C/S 模式中，WWW 服务成为核心服务，用户通过浏览器访问资源。而随着浏览器技术的发展，用户通过浏览器不仅能进行超文本的浏览查询，而且还能收发电子邮件，进行文件的上传和下载等工作。也就是说，用户在浏览器统一的接口上能完成网络上各种服务和应用功能。

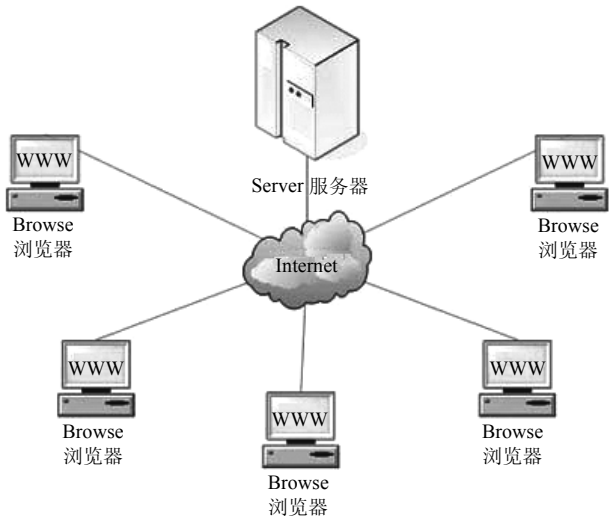



图 4-27　B/S 网络模式

B/S 模式的主要特点：

（1）浏览器/服务器模式是一种平面型多层次的网状结构。网络用户在基于浏览器的客户机上以网络用户界面（NUI）多对多地访问应用服务器上的资源。用户访问应用服务器资源以动态交互或相互合作的方式进行；

（2）B/S 计算模式最主要的特点是与软、硬件平台的无关性，浏览器、Web-Server、Java、HTML 以及数据库资源都可以做到与软、硬件平台无关；

（3）在 B/S 模式下，可以将应用逻辑和业务处理规则放置在服务器一侧，对于这样的结构，客户机可以做得尽可能“瘦”，其功能可能仅体现在一个浏览器或是 Java 虚拟机上；

（4）分散应用与集中管理；

（5）系统易维护性。

## 4.5　典型局域网

目前常见的局域网类型包括：以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式数据接口（FDDI）、异步传输模式（ATM）等。而最具代表性的是以太网。

以太网是基于总线型的广播式网络，采用 CSMA/CD 媒体访问控制方法。以太网最早是 1975 年由美国 Xerox（施乐）公司研制成功，以历史上表示传播电磁波的以太（Ether）命名的网络。以太网最初采用的是总线形结构，用无源介质（如同轴电缆）作为总线来传输信息，现在采用星形结构。以太网费用低廉、便于安装、操作方便，因此得到广泛的应用。

### 4.5.1　传统以太网

在已有的局域网标准中，以太网是最成功的局域网技术，也是当前应用最广泛的一种局域网。从它的应用领域来看，以太网不仅是局域网的主流技术，而且采用以太网技术组建城

域网也已成熟。在我国以太网技术正进入家庭联网领域。所以无论从计算机网络发展的历史，还是从网络技术未来的发展前景看，都不难得出这样的结论：以太网技术是极为重要的，它不仅是局域网和城域网的主流技术，而且以太网技术在广域网应用方面也在发挥它的作用。

传统以太网是 10Mbps，使用 CSMA/CD 媒体访问控制方法。物理层标准主要包括基带以太网 10Base-5、10Base-2、10Base-T 和 10Base-F，另外还有宽带以太网技术 10Broad36。下面主要介绍基带以太网。

### 1．10Base-5 标准

10Base-5 以粗铜轴电缆为传输介质，常被称为粗缆以太网。其网络结构如图 4-28 所示。

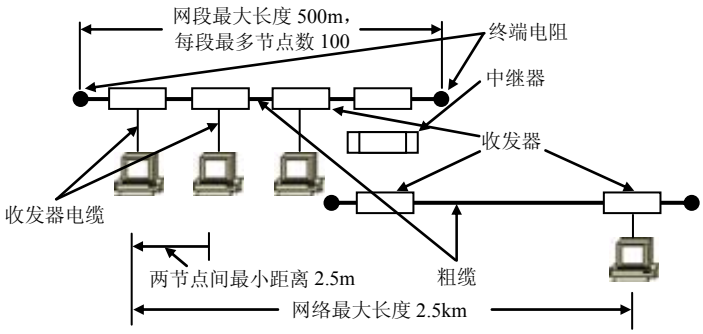



图 4-28　10Base-5 网络结构

10Base-5 网络结构主要包括以下几个部分：

（1）粗同轴电缆（Coaxial Thick Cable）它是特性阻抗为 50Ω的基带粗同轴电缆，直径 10mm。

（2）收发器（Transceive）又称外部收发器，它需要牢牢地夹在电缆上，使得触针能接触到电缆的内芯。收发器内部有电子线路进行载波监听和冲突检测。当检测到冲突时，收发器就在电缆上产生一个特殊的无效信号，确保其他收发器也能知道冲突的产生。

（3）收发器电缆（Transceive Cable）它是连接网卡和收发器的多芯电缆，通常又称为 AUI 电缆。AUI 是指连接单元接口（Attachment Unit Interface），它使用 DB-15 连接器。

（4）网卡（Network Interface Card）支持粗缆以太网的网卡上都带有 AUI 接口，以便和收发器电缆相连。

（5）终接器（Terminal Connector）每条电缆必须在两端接上 50Ω的终接器（终端匹配器），它的主要作用是：当信号到达电缆两端时，把信号全部吸收，以避免信号反射。

10Base-5 的技术规范：

（1）两台相邻计算机（收发器）之间的最小距离为 2.5m；

（2）最大干线（接收发器）长度为 500m；

（3）一个网段的最大长度不能超过 500m；

（4）一个网段上最多可连接的计算机数为 100 台；

（5）最大网段数是 5 个（即用 4 个中继器来连接）；

（6）最大网络干线电缆长度为 2 500m。

### 2．10Base-2 标准

用基带细同轴电缆组建的网络称为细缆以太网，又可表示为 10Base-2，其网络结构如图 4-29 所示。

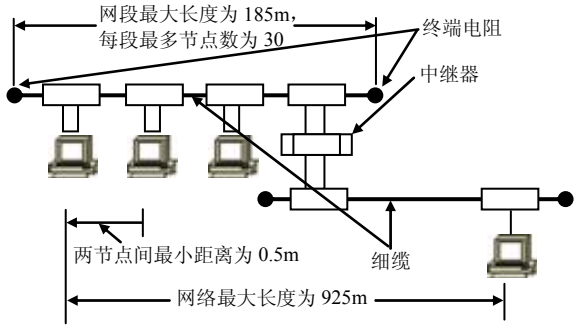



图 4-29　10Base-2 网络结构

10Base-2 标准的技术规范如下：

（1）两台相邻计算机之间的最小距离为 0.5m。（在实际建网时，一般建议两台相邻计算机之间距离大于 1m）；

（2）一个网段的最大长度不能超过 185m；

（3）一个网段上最多可连接的计算机数为 30 台；

（4）最大网段数是 5 个（即用 4 个中继器来连接）；

（5）最大网络干线电缆长度为 925m。

由于 10Base-5 和 10Base-2 网络不便管理和维护，目前已逐步被淘汰。

### 3．10Base-T 标准

10Base-T 是由 IEEE 802 委员会经过 3 年的研究，11 次修改，终于在 1990 年 9 月正式批准的使用无屏蔽双绞线传输 10Mbps 基带信号的以太网标准。使用集线器的 10Base-T 网络，它实际是一个物理上为星形连接，逻辑上为总线形拓扑的网络。其结构如图 4-30 所示。

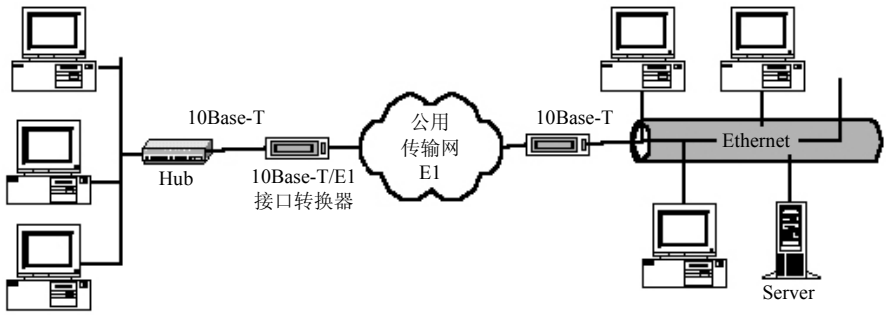



图 4-30　10Base-T 网络结构

10Base-T 的组成：

（1）双绞线连接器（Twisted pair Connector）采用标准的 RJ-45 连接器，共有 8 芯。

（2）双绞线（Twisted Pair）10Base-T 通常使用非屏蔽双绞线（UTP），在双绞线两端各使用一个 RJ-45 连接器。

（3）集线器（Hub）是 10Base-T 以太网的核心，也称为网络中心部件。它相当于一个多端口的中继器，且端口通常使用 RJ-45 端口，其端口数量可以是 8、12、16 或 24。另外，有些集线器上还带有与同轴电缆相连接的端口（AUI、BNC）及与光纤相连接的端口。

（4）网卡（Network Interface Card）在网卡上应有一个连接双绞线的 RJ-45 端口。另外支持 10Base-T 的网卡对输出信号应进行前置补偿，以抵消双绞线频带窄所造成的信号失真。

1990 年，由 IEEE 802 公布了 10Mbps 双绞线以太网标准 10Base-T，编号为 IEEE 802.3i。该标准规定在非屏蔽双绞线（UTP）介质上提供 10Mbps 的数据传输速率。每个网络站点都需要通过 UTP 连接到一个中心设备集线器（Hub）上，构成星形拓扑结构。10Base-T 双绞线以太网系统操作在 2 对 3 类 UTP 上，一对用于发送信号，另一对用于接收信号。为了改善信号的传输特性和信道的抗干扰能力，每一对线必须绞在一起。“5—4—3”原则也适用于 10Base-T 网络，即最多 5 个网段，连接 4 个中继器（或集线器），两个节点之间经过的有计算机的网段最多为 3 个。

10Base-T 的主要技术规范如下：

（1）数据的传输速率为 10Mbps，基带传输；

（2）每段双绞线最大长度为 100m（Hub 与工作站间及两个 Hub 之间）；

（3）一条通路最多允许连接的 Hub 数为 4 个；

（4）物理拓扑结构为星形。逻辑拓扑结构为总线形；

（5）访问控制方式为 CSMA/CD；

（6）帧长度为可变，最大为 1 518 字节；

（7）最大传输距离为 500m；

（8）每个网段上的最大节点数为 512 个。

10Base-T 的连接主要以集线器 Hub 作为枢纽，工作站通过网卡的 RJ-45 插座与 RJ-45 接头相连，另一端 Hub 的端口都可供 RJ-45 的接头插入，拆装非常方便。

10Base-T 由于安装容易，价格比粗缆和细缆都便宜，管理、连接方便，性能优良，一经问世就受到广泛注意和大量的应用，归结起来它有如下特点。

（1）网络建立和扩展十分灵活方便。根据每个 Hub 的端口数量（有 4、8、12、16 口）和网络大小选用不同端口的 Hub，构成所需网络；增减工作站时可不中断整个网络的工作；可以预先和电话线统一布线，并在房间内预先安装好 RJ-45 插座，所以改变网络布局十分容易。

（2）Hub 具有自动隔离故障作用。当某工作站发生故障时，不会影响网络的正常工作；Hub 可将一个网络有效地分成若干互连的段，当发生故障时，管理人员可在较短时间内迅速查出故障点，提高故障排除的速度，故使用场合较多。

### 4．10Base-F 标准

10Base-F 是 10Mbps 光纤以太网，它使用多模光纤传输介质，在介质上传输的是光信号而不是电信号。因此，10Base-F 具有传输距离长、安全可靠、可避免电击的危险等优点。由于光纤介质适宜连接相距较远的站点，所以 10Base-F 常用于建筑物间的连接，它能够建园区主干网（如北京大学早期的校园主干网采用的就是 10Base-T 技术），并能实现工作组级局域网与主干网的连接。

由于光纤的带宽很宽，10Base-F 只用了很小一部分，不经济，故该标准现已被淘汰。

### 4.5.2 快速以太网

为了满足网络应用对带宽的需求，开发一种简单、实用、能普遍应用于桌面系统的快速局域网技术，IEEE 802.3 委员会于 1992 年提出制定快速以太网标准。在 IEEE 802.3 基础上，把传输速率提高到 100Mbps，并于 1995 年 6 月正式把它定为快速以太网标准 IEEE 802.3u。

快速以太网的数据传输速率为 100Mbps。它保留着传统 10Mbps 速率 Ethernet 的所有特征，即相同的数据格式、相同的介质访问控制方法 CSMA/CD 和相同的组网方法，而只是把每个比特发送时间由 100ns 降低到 10ns。Fast Ethernet 遵循的标准是 100Base-T。

100Base-T 标准不但在最大程度上保持了 IEEE 802. 3 标准的完整性，而且保留了核心以太网的细节规范。

#### 1．100Base-T 主要特点

（1）采用与 10Base-T 相似的层次协议结构，其中 LLC 子层完全相同；

（2）帧格式与 10Base-T 相同，包括最小帧长为 64 字节，最大帧长为 1 518 字节，帧间最小间隙为 12 字节；

（3）MAC 子层与物理层之间采用介质无关接口 MII；

（4）介质访问控制方法为 CSMA / CD；

（5）拓扑为以 100Base-T 集线器 / 交换机为中心的星形拓扑结构；

（6）传输速率为 100Mbps；

（7）传输介质为 UTP 或光纤；

（8）网络最大直径为 205m。

#### 2．100Base-T 物理层规范

根据网络所使用的传输介质的不同，100Base-T 定义了 100Base-TX、100Base-T4 和 100Base-FX 3 种不同的物理层规范。

（1）100Base-TX：100Base-TX 采用两对五类 UTP 或两对一类 STP 作为传输介质，其中一对用于发送；另一对用于接收，站点与集线器之间的最大距离为 100m。对于五类 UTP，使用 RJ-45 连接器；对于一类 STP 使用 DB-9 连接器。

（2）100Base-T4：100Base-T4 采用 4 对三类、四类和五类 UTP 作为传输介质。4 对线中，3 对用于数据传输，1 对用于冲突检测。使用 RJ-45 连接器，站点与集线器之间的最大距离为 100m。

（3）100Base-FX：100Base-FX 采用两束多模光纤作为传输介质，每束都可用于两个方向，因此它是全双工的，并且在每个方向上速率均为 100Mbps。适用于高速主干网、有电磁干扰环境、要求通信保密性好和传输距离远等应用场合，使用标准 FDDI MIC 连接器、ST 连接器和 SC 连接器，站点与集线器之间的最大距离高达 2km。

#### 3．组网规则

（1）各网络站点需通过 Hub（100Mbps）连到网络中；

（2）传输介质用 5 类非屏蔽双绞线或 150Ω屏蔽双绞线；

（3）双绞线与网卡与 Hub 之间的连接，可使用 8 针 RJ-45 标准连接器；

（4）网络站点与 Hub 之间的最大距离长度为 100m。

在一个冲突域中只能连接一个Ⅰ类 Hub，网络的最大直径（站点—Hub—站点）为 200m。如果使用Ⅱ类集线器，最多可以级连两个 Hub，网络的最大直径（站点—Hub—Hub—站点）为 205m。100Base-T 的网络结构如图 4-31 所示。

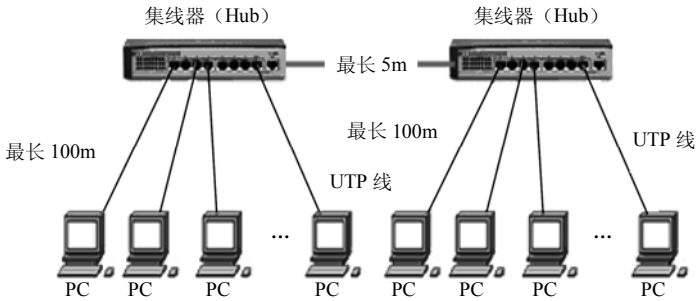



图 4-31　100Base-T 的网络结构

## 4.5.3　高速以太网

尽管快速以太网 Fast Ethernet 具有高可靠性、易扩展性、低成本等优点，并且成为高速局域网方案中的首选技术，但由于多媒体通信和视频技术的广泛应用、电子商务和信息高速公路及智能大厦的发展、科研和教育的宽带网络化等，使人们不得不寻求更高带宽的局域网。千兆位和万兆位以太网就是在这种背景下产生的。

### 1．千兆位以太网

与快速以太网 Fast Ethernet 相同之处是：千兆位以太网同样保留着传统的 100Base-T 的所有特征，即相同的数据格式、相同的介质访问控制方法 CSMA/CD 和相同的组网方法，而只是把 Fast Ethernet 每个比特的发送时间由 10ns 降低到 1ns。根据所使用介质的不同，高速以太网具有多种不同的物理层规范，基于光纤的千兆位以太网标准是 IEEE 802.32；基于 5 类 UTP 的千兆位以太网标准是 IEEE 802.3ab。

千兆位以太网的物理层标准主要包括 1000Base-SX、l000 Base-LX、1000Base-CX 和 1000Base-T。

（1）1000Base -SX 标准：1000Base -SX 是一种使用短波激光作为信号源的网络介质技术，波长为 770～860nm（一般为 850nm）的激光传输器，它不支持单模光纤，只能驱动多模光纤。它所使用的光纤规格有两种：芯径为 62.5μm 和 50μm 的多模光纤，采用 8B/10B 编码方式，传输距离分别为 260m 和 525m，适用于建筑物中同一层的短距离主干网。

（2）1000 Base-LX 标准：1000 Base-LX 是一种使用长波激光作为信号源的网络介质技术，配置波长为 1 270～1 355nm（一般为 1 300nm）的激光传输器，它既可以驱动多模光纤，也可以驱动单模光纤。它所使用的光纤规格为：纤芯为 62.5μm 和 50μm 的多模光纤，工作波长为 850nm，传输距离为 525m 和 550m，数据编码方法为 8B/10B，适用于作为大楼内部网络系

统的主干网；纤芯规格为 9μm 的单模光纤，工作波长为 1 300nm 或 1 550nm，传输距离为 3 000m，适用于校园或城域主干网。

（3）1000 Base -CX 标准：1000 Base -CX 使用 150Ω屏蔽双绞线（STP），采用 8B /10B 编码方式，传输速率为 1.25Gbps，传输距离为 25m，主要用于集群设备的连接，如一个交换机机房内的设备互连。

（4）1000Base-T 标准：使用 4 对 5 类非屏蔽双绞线（UTP），传输距离为 100m，主要用于结构布线中同一层建筑内的通信，可以利用以太网或快速以太网已铺设的 UTP 电缆，在以太网系统中实现从 100～1 000Mbps 的平滑升级。

2．万兆位以太网

随着以太网采纳程度的增长，今天在局域网部署中已达到 95%的水平，为满足更高带宽、光纤安装及地域更广大的网络需要，万兆位以太网应运而生。

万兆位以太网 802.3ae 标准由 IEEE 于 2002 年 6 月批准，而且现在已在许多应用中进入大量部署阶段。万兆位以太网作为以下技术的核心技术同样重要，即服务器室内交换、城域接入和回程网络以及利用原有 SONET/SDH 设备的长途安装。

在从千兆位以太网到万兆位以太网的演变过程中，为了适合如此广泛的可能应用，已进行了大量更改。这些更改中，最重要的更改与数据编码方式及万兆位以太网可以运行的物理连接类型有关。帧尺寸和格式都保持不变，以便第 3 层及更高层协议仍然完全兼容。

万兆位以太网设计用于以全双工模式只在点到点（交换）链路上运行。这一点反映其作为主干（与工作组不同）技术的角色。万兆位以太网当前不支持自动协商，因为它被假定用于纯万兆位以太网安装。万兆位以太网标准引入了新的 64B/66B 编码方案，使传输速率接近 10Gbps。这允许系统制造商利用最初为 SONET/SDH 应用开发的成熟的 10Gbps 技术。当前，万兆位以太网已批准用于光纤线路，铜线规范正在由 IEEE 审查。

### 4.5.4 ATM 网

ATM（Asynchronous Transfer Mode）指异步传输模式，它是为高速数据传输和通过公共网或专用网传输多种业务数据而设计的。这是一种以小的、固定长的包（Cell，信元）为传输单位，面向连接的分组交换技术。ATM 是在 1989 年产生的，后被国际电讯联盟标准化组织 ITU-T 确定为传输语音、图像、数据和多媒体信息的工具。虽然开发 ATM 的原意是希望用于宽带综合业务数据网（B-ISDN），但由于实施的复杂性，ATM 最终被用于局域网。近几年来，ITU-T、ATM 论坛、ANSI、ETSI（欧洲电信标准协会）和 IETF（Internet 工程任务组）等标准化组织为 ATM 定义了一系列标准，使 ATM 技术在局域网建设中很快被推广应用，现在 ATM 已成为局域网主干网的主流技术之一。

ATM 是近几年来新兴的网络技术，它的主要特点如下：

（1）面向连接的分级交换技术，综合了电路交换和分组交换的优点；

（2）以小的、固定长度的信元（cell）为基本传输单位，每个信元的延迟时间是可预计的；

（3）允许声音、视频、数据等多种业务信息在同一条物理链路上传输，它能在一个网络

上用统一的方式综合多种业务服务；

（4）数据传输速率高，可达 25Mbps～20Gbps，常用的为 155.52Mbps、622.08Mbps；

（5）为星形拓扑结构，并可构造网状拓扑结构；

（6）提供质量保证 QoS 服务。ATM 为不同的业务类型分配不同等级的优先级，如为视频、声音等对时延敏感的业务分配高优先级和足够的带宽；

（7）是一种局域网与广域网的综合技术，能实现 LAN 和 WAN 的无缝连接；

（8）传输介质可以是光纤（单模、多模）或双绞线（如五类双绞线）。

通过局域网仿真，ATM 可以和现有以太网、令牌环网共存。由于 ATM 网与以太网等现有网络之间存在着很大差异，所以必须通过 LANE、MPOA 和 IPOver ATM 等技术，它们才能结合，而这些技术会带来一些局限性，如影响网络性能和 QoS 服务等。

ATM 网络具有很好的扩充能力，易升级、易扩展。

为了满足以更高的速率传输多种业务信息的需要，ATM 采用了更有效地传输技术，它的基本技术是信元交换和面向连接。

#### 1．信元交换

ATM 的基本思想是将数据分割成小的、固定长度的包，称为信元，然后，以信元为基本传输单位，通过信元交换机（ATM Switching）转发它们，实现信元交换。每个信元有 53 字节，包括 5 字节信元头和 48 字节净荷（payload），即数据信息。由于信元是固定长度，且信头又很简单，所以 ATM 网络能够用硬件实现信元的快速转发，以及对时间延迟和时延抖动要求严格的业务类型的数据传输，并能充分利用物理层资源。

#### 2．面向连接

在 ATM 网络中，两个站点想进行通信对话时，首先要在它们之间建立连接，即建立一条虚拟通道。该连接一直保留到对话结束才关闭，对于用户而言，这个连接一旦建立就是永久的，但实际上不是。在 ATM 中建立连接意味着选择一条从源头到目的地的路径，以便传输信元。因为通过 ATM 传输信息，必须先建立连接，所以 ATM 是一种面向连接的技术。

### 4.5.5　FDDI 网

FDDI 的中文意思是光纤分布式数据接口，是计算机网络技术发展到调整通信阶段的第一个高速网络技术。FDDI 是由美国国家标准协会 ANSI X3T9.5 委员会确定的一种使用光纤作为传输介质的、高速的、通用的令牌环网，后来又通过了国际标准 ISO 9314。

#### 1．FDDI 网的网络拓扑结构

FDDI 采用主、副双环结构，主环进行正常的数据传输，副环为冗余的备用环。它的速率为 100Mbps，网络覆盖的最大距离可达 200km，最多可连接 1 000 个节点。

一个 FDDI 一般包括光纤、工作站、集线器和网卡等部分。在 FDDI 上所连接的工作站有 A 类站或双附接站（DAS）和 B 类站或单附接站（SAS）两类。凡是要直接连接到 FDDI 网上的设备，都应配置 FDDI 网卡。FDDI 网卡分为双附接网卡和单附接网卡两种。FDDI 网的基本结构如图 4-32 所示。

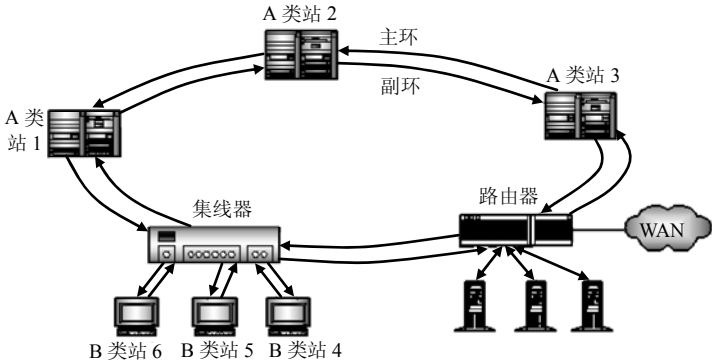



图 4-32　FDDI 网络的基本结构

### 2．FDDI 介质访问控制方式

FDDI 所采用的介质访问控制方式与 IEEE 802.5 标准中的对应部分相似。所不同的是 802.5 中采用的是单数据帧访问方式；而在 FDDI 中则采用的是多数据帧访问方式，即允许在环路中同时存在着多个数据帧，可提高信道利用率。

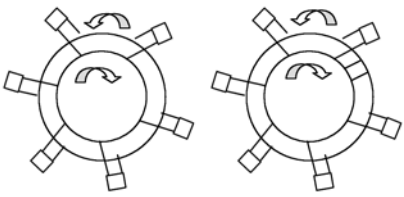


图 4-33　FDDI 的自愈功能

### 3．FDDI 的自愈功能

FDDI 采用主、副双环结构，主环进行正常的数据传输，副环为冗余的备用环。当主环在某处断开时，副环能自动和主环连通，形成一个新的环状结构，如图 4-33 所示。这种自愈功能大大提高了 FDDI 数据传输的可靠性。

## 4.5.6　无线局域网

通常计算机组网的传输媒介主要依赖铜缆或光纤，构成有线局域网。但有线网络在某些场合要受到布线的限制：布线、改线工程量大；线路容易损坏；网中的各节点不可移动。特别是要把相距较远的节点连接起来时，铺设专用通信线路的布线施工难度大、费用高、耗时长，对正在迅速扩大的联网需求形成了严重的瓶颈阻塞。无线局域网（Wireless LAN，WLAN）就是为解决有线网络的以上问题而出现的。

无线局域网与传统以太网相比具有以下优点。（1）安装便捷；（2）使用灵活；（3）经济节约；（4）易于扩展。

由于 WLAN 具有多方面的优点，其发展十分迅速。在最近几年里，WLAN 已经在医院、商店、工厂和学校等不适合网络布线的场合得到了广泛的应用。

无线局域网使用的是无线传输介质，按照所采用的传输技术可以分为 3 类：红外线局域网、扩频无线局域网和窄带微波无线局域网。

### 1．红外线局域网

红外线也是按视距方式传播的，也就是说发送点可以直接看到接收点，中间没有阻挡。红外线相对于微波传输方案来说有一些明显的优点。首先，红外线频谱是非常宽的，所以就

有可能提供极高的数据传输速率。由于红外线与可见光有一部分特性是一致的，所以它可以被浅色的物体漫反射，这样就可以用天花板反射来覆盖整个房间。红外线不会穿过墙壁或其他的不透明物体，因此红外线无线局域网具有以下几个优点：

（1）红外线通信比起微波通信不易被入侵，由此提高了安全性；

（2）安装在大楼中每个房间里的红外线网络可以互不干扰，因此建立一个大的红外线网络的设想是可行的；

（3）红外线局域网设备相对简单且便宜。红外数据传输基本上是用强度调制，所以红外接收器只要测量光信号的强度，而大多数微波接收器则要测量信号的频谱或相位。

### 2．扩频无线局域网

目前，最普遍的无线局域网技术是扩展频谱（简称扩频）技术。扩频技术开始是为了军事和情报部门的需求开发的，其主要想法是将信号散布到更宽的带宽上，以使发生拥塞和干扰的概率减小。扩频的第一种方法是跳频（Frequency Hopping）；第二种方法是直接序列（Direct Sequence）扩频。这两种方法都被无线局域网所采用。

（1）跳频：在跳频方案中，发送信号频率按固定的间隔从一个频谱跳到另一个频谱。接收器与发送器同步跳动，从而保证正确地接收信息。而那些可能的入侵者当没有找到跳频规律时，只能得到一些无法理解的标记。

IEEE 802.11 标准规定每 300ms 的间隔变换一次发送频率。发送频率变换的顺序由一个伪随机码决定，发送器和接收器使用相同变换的顺序序列。数据传输可以选用频移键控或二进制相位键控方法。

（2）直接序列扩频：在直接序列扩频方案中，输入数据信号进入一个通道编码器并产生一个接近某中央频谱的较窄带宽的模拟信号。这个信号将用一系列看似随机的数字（伪随机序列）来进行调制，调制的结果大大地拓宽了要传输信号的带宽，因此称为扩频通信。在接收端，使用同样的数字序列来恢复原信号，信号再进入通道解码器来还原传送的数据。

### 3．窄带微波无线局域网

窄带微波（Narrowband Microwave）是指使用微波无线电频带来进行数据传输，其带宽刚好能容纳信号。以前所有的窄带微波无线网产品都使用申请执照的微波频带，直到最近制造商才开始提供在工业、科学和医药频带内的窄带微波无线网产品。

（1）申请执照的窄带 RF：每个地理区域的半径为 28km，并可容纳 5 个执照，每个执照覆盖两个频率范围。申请执照的窄带无线网的优点是，它保证了无干扰通信。

（2）免申请执照的窄带 RF：1995 年，Radio LAN 成为第一个使用免申请执照 ISM 的窄带无线局域网产品。1990 年 IEEE 802 委员会成立了 IEEE 802.11 工作组，专门从事无线局域网的研究，并于 1997 年由大量的局域网及计算机方面的专家审定通过 IEEE 802.11 无线局域网标准。IEEE 802.11 规定了无线局域网在 2.4GHz 波段进行操作，这一波段被全球无线电法规实体定义为扩频使用波段。

1999 年 8 月，802.11 标准得到了进一步的完善和修订，一种是 802.11a，它扩充了标准的物理层，频带为 5GHz，采用 QFSK 调制方式，传输速率为 6～54Mbps。它采用正交频分复用的独特扩频技术，可提供 25Mbps 的无线 ATM 接口和 10Mbps 的以太网无线帧结构接口；另一种是 802.11b 标准，采用 2.4GHz 频带和补偿编码键控调制方式。该标准可提供 11Mbps 的

数据速率，且可以根据情况的变化，在 11Mbps、5.5Mbps、2Mbps、1Mbps 等不同速率之间自动切换。它从根本上改变了 WLAN 设计和应用现状，扩大了 WLAN 的应用领域，现在，大多数厂商生产的 WLAN 产品都基于 802.11b 标准。

图 4-34 是由以太网交换机、服务器、无线访问点（无线路由器）、装有无线网卡的主机等组成的一个有线网络和无线网络互连的网络结构，是一个使用的中小型办公室无线网络的解决方案。

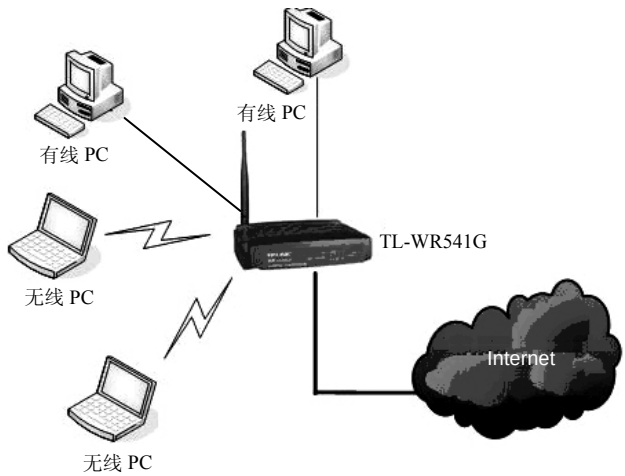



图 4-34　一个办公室无线网络的解决方案

## 4.6　交换式局域网

以太网、快速以太网、FDDI 和令牌环网常被称为传统局域网，它们都是共享介质、共享带宽的共享式局域网。所谓共享式网络就是在网络上的所有站点共享一条传输通道，在任一时刻只有一个节点发送信息，其他节点接收信息并通过对信头的分析来判定是不是发给自己的。由于 CSMA/CD 协议对冲突的处理极大地影响了网络效率，尤其是在网络负载重时，大量的冲突和重发，会使网络效率急剧下降。所以以太网的带宽利用率一般为 30%左右。

共享式局域网还具有共享带宽的特性，网上的每个站点只能得到局域网带宽的一小部分。如以太网的带宽为 10Mbps，则对于 100 个节点的网络，理论上每个节点分享的带宽只有 0.1Mbps，这就使得网络规模扩大时，整体效率下降，延迟增加，所以共享式局域网不能提供足够的带宽。

传统局域网为了提高带宽，往往使用路由器进行网络分割，将一个网络分为多个网段，每个网段有不同的子网地址，不同的广播域，以减少网络上的冲突，提高网络带宽。这种方法称为网络微段化或微化网络。网络微段化是指将一个较大的网分为几个或几十个网段，这就使得网络结构和网络管理变得十分复杂且成本提高，而且也不能根本解决网络带宽的问题。而交换式局域网技术，能够解决共享式局域网所带来的网络效率低、不能提供足够的网络带宽和网络不易扩展等一系列问题，它从根本上解决了带宽问题。

以太网交换技术是在多端口网桥的基础上于 20 世纪 90 年代初发展起来的。交换式局域

网的核心是交换式集线器 Switch（也称交换机），其主要特点是：所有端口平时都不连通；当站点需要通信时，交换机才同时连通许多对端口，使每一对相互通信的站点都能像独占通信信道那样，进行无冲突地传输数据，即每个站点都能独占信道速率；通信完成后就断开连接。因此，交换式网络技术是提高网络效率、减少拥塞的有效方案之一。

### 4.6.1　交换式局域网的基本特点

交换式局域网是指以数据链路层的帧或更小的数据单元（信元）为数据交换单位，以交换设备为基础构成的网络。交换式网络的核心设备是交换机。交换机为每个端口提供专用的带宽，各个站点有一条专用链路连接到交换机的一个端口，这样每个站点都可以独享通道，独享带宽。

交换式局域网主要有以下几个特点：

（1）独占传输通道，独占带宽。交换式局域网把“共享”变为“独享”，网络上的每个站点都能独占一条点到点的通道。网络的总带宽通常为各个交换端口带宽之和。所以在交换式网络中，随着用户的增多，网络带宽在不断增加，而不是减少。当然这只是针对局域网而言，如将这个局域网接入广域网，那出口带宽又另当别论。

（2）允许多对站点同时通信。共享式局域网中，在介质上是串行传输，任何时候只允许一个帧在介质上传送。交换机是一个并行系统，它可以使接入的多个站点之间同时建立多条通信链路，让多对站点同时通信，所以交换式网络大大地提高了网络的利用率。

（3）灵活的接口速度。在共享式网络中，不能在同一个局域网中连接不同速率的站点（如 10Base-5 仅能连接 10Mbps 的站点）。而在交换网络中，由于站点独享介质，独享带宽，用户可以按需配置端口速率。在交换机上可以配置 10Mbps、100Mbps、10Mbps/100Mbps 自适应端口，用于连接不同速率的站点，接口速度有很大的灵活性。

（4）高度的可扩充性和网络延展性。大容量交换机有很高的网络扩展能力，而独享带宽的特性使扩展网络没有带宽下降的后顾之忧。因此，交换式网络可以是一个大规模的网络，如大的企业网、校园网或城域网。

（5）交换式局域网可以与现有网络兼容。如交换式以太网与以太网和快速以太网完全兼容，它们能够实现无缝连接。

（6）互连不同标准的局域网。局域网交换机具有自动转换帧格式的功能，因此它能够互连不同标准的局域网，如在一台交换机上能集成以太网、FDDI 和 ATM。

### 4.6.2　交换机的基本工作原理

#### 1．局域网交换机的工作原理

典型的局域网交换机结构与工作过程如图 4-35 所示。交换机的每个端口内部都配有缓冲器，使交换机可以以存储/转发方式工作。交换机的内存中有一张地址表（地址转发表），反映了交换机的端口号和该端口上所连接的主机网卡的 MAC 地址之间的对应关系。

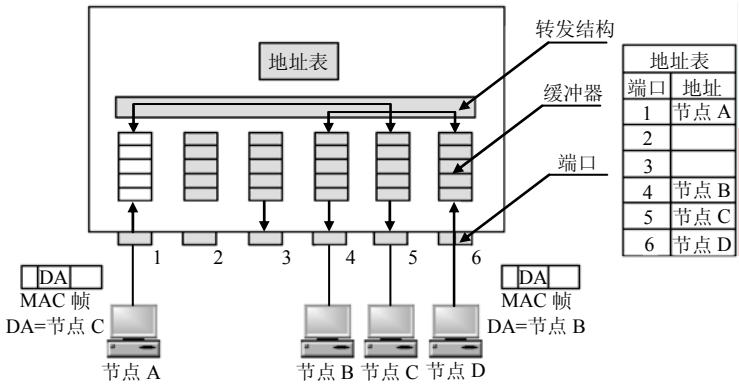



图 4-35　交换机的结构

当连在交换机上的某主机发送信息时，交换机会从缓冲器中读出源 MAC 地址，与端口号一起填入地址表中，当所有连接在交换机上的主机都发送过信息时，就会形成一张完整的地址转发表，如图 4-36 所示。

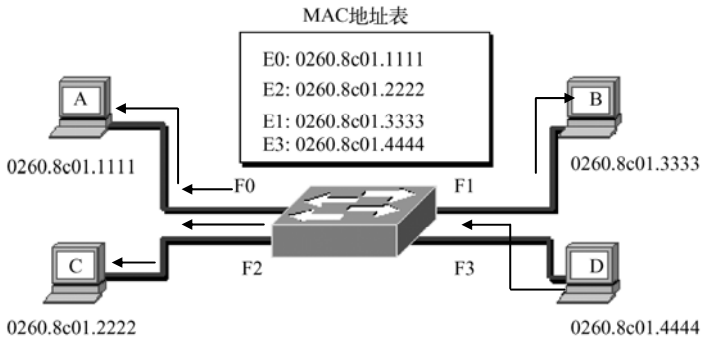



图 4-36　交换机的工作原理

交换机某端口接收到一个数据帧时，它从缓冲区中取出目的 MAC 地址，通过查找地址表获取目标主机所接收端口号，转发机构通过背板将源端口和目的端口连通以实现数据转发。这种端口之间的连接可以根据需要同时建立多条，也就是说可以在多个端口之间建立多个并发连接。

当交换机接收到一个广播帧或目的端口未知的单播帧时，会像集线器一样工作，即向所有端口转发。

### 2．交换机的帧转发方式

以太网交换机的帧转发方式可以分为以下三类：

（1）直接交换方式：在直接交换（Cut Through）方式中，交换机只要接收并检测到目的地址，立即将该帧转发出去，而不管这一帧数据是否出错。帧出错检测任务由节点主机完成。这种交换方式的优点是交换延迟的时间短，缺点是缺乏差错检测功能，不支持不同输入/输出速率的端口之间的帧转发。

（2）存储转发交换方式：在存储转发（Store and Forward）方式中，交换机首先完整地接收发送帧，并先进行差错检测。如果接收帧是正确的，则根据帧的目的地址确定输出端口号，然后再转发出去。这种交换方式的优点是具有帧差错检测能力，并能支持不同输入/输出速率

的端口之间的帧转发，缺点是交换延迟时间将会增长。

（3）改进的直接交换方式：改进的直接交换方式则将两者结合起来，它在接收到帧的前 64 字节后，判断 Ethernet 帧的帧头是否正确，如果正确则转发出去。这种方法的优点是能有效地防止小于 64 字节的垃圾数据，并有交换延时短的特点，缺点是只对帧头进行校验，而对数据部分无校验功能。

### 3．冲突域与广播域

由于交换机对所有端口转发广播信息，所以交换机连成的网络属于同一广播域。

只有当多个端口争用同一端口或某个接口直接连接了一个集线器，而集线器又连接了多台主机时，交换机上的该接口和集线器上所连的所有主机才可能产生冲突，形成冲突域。换句话说，交换机上的每个接口都是自己的一个冲突域，如图 4-37 所示。

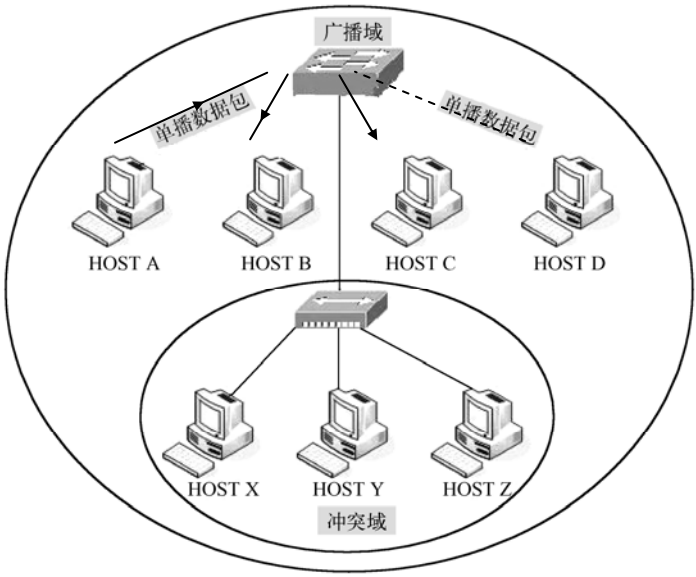



图 4-37　冲突域与广播域

## 4.6.3　交换机的管理及基本配置方法

### 1．交换机的管理方式

交换机的管理可分为带外管理和带内管理。

（1）带外管理：通过交换机上的配置端口（Console 口）对交换机进行管理。这种方法不占用交换机的基本带宽，因此叫带外管理。

（2）带内管理：通过交换机的普通端口对交换机进行管理，这种方法要占用交换机的基本带宽，故叫带内管理。带内管理常用的方法有 3 种，分别是：

① 通过 Telnet 对交换机进行远程管理；

② 通过 Web 对交换机进行远程管理；

③ 通过 SNMP 工作站对交换机进行远程管理。


图 4-38　配置超级终端

### 2．带外交换机的配置方法

（1）连接：用全反线连接配置主机的 COM 口和交换机的 Console 口。

（2）打开超级终端：选择“开始”→“程序”→“附件”→“通信”→“超级终端”命令，进入并打开超级终端程序。

（3）配置超级终端：包括为连接命名、选择合适的 COM 口、配置正确的参数（如图 4-38 所示）。

当完成上述步骤后，即可进入交换机的配置界面。

### 3．交换机的基本命令

（1）交换机的工作模式。

| 工作模式 | 提示符 | 该模式下可完成的功能 |
|---|---|---|
| 用户模式 | Switch> | 交换机信息的查看，简单测试命令 |
| 特权模式 | Switch# | 查看、管理交换机配置信息， |
| 全局配置模式 | Switch（config）# | 配置交换机的整体参数 |
| 接口配置模式 | Switch（config-if）# | 配置交换机的接口参数 |
| VLAN 配置模式 | Switch（config-vlan）# | 配置 VLAN 信息 |

（2）命令使用举例。

```
Switch> enable 14                                  用 14 级密码进入特权模式
Switch#  configure terminal                        进入全局配置模式
Switch（config）# interface fastethernet 0/1       进入端口配置模式
Switch（config-if）# exit                          返回上一模式
Switch（config-if）# end                           直接返回特权模式
Switch# disable                                    返回用户模式
```

（3）命令行其他功能：包括获得帮助、命令简写和使用历史命令等操作。

① 获得帮助：例：

```
Switch#?              ; 列出当前模式下所有可用的命令
Switch#sh?            ; 列出当前模式下以 sh 开头的所有可用命令
Switch#show  ?        ; 列出当前模式下 show 为第一个单词的所有可用命令
```

② 命令简写：例：

```
全写：Switch# configure terminal
简写：Switch# config
```

③ 使用历史命令：可用向上键（↑）或向下键（↓）选择曾经使用过的命令。

（4）配置交换机 Telnet 功能：包括配置远程登录密码、配置进入特权模式密码和为交换机配置管理 IP 等操作。

配置远程登录密码：

```
Switch(config)#enable secret level 10  ruijie
```

配置进入特权模式密码：

```
Switch(config)#enable secret level 150  ruijie
```

为交换机配置管理 IP：

```
Switch(config)#interface vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#end
```

# 4.7　虚拟局域网

## 4.7.1　虚拟局域网概述

在传统的局域网中，通常一个工作组是在同一个网段上，每个网段可以是一个逻辑工作组或子网。多个逻辑工作组之间通过实现互联的网桥或路由器来交换数据。如果一个工作组中的一个节点要转移到另一个工作组时，就需要将节点计算机从一个网段撤出，连接到另一个网段上，甚至需要重新进行布线。因此，逻辑工作组的组成就要受节点所在网段的物理位置限制。

虚拟局域网（VLAN）是以交换式网络为基础，把网络上的用户（终端设备）用软件的方法分为若干个逻辑工作组或逻辑子网，每个逻辑工作组就是一个 VLAN。

VLAN 并不是一种新型的局域网技术，而是交换网络为用户提供的一种服务。它允许网络管理员使用软件实现按业务功能、网络应用、组织机构或其他任何需要，灵活地划分逻辑子网，增加或删除子网成员。同一虚拟网中的成员不受物理的位置限制，也就是说虚拟网的划分与用户所处的位置无关，组中的成员可以不在同一个物理网段上，当终端设备移动时，无须修改它的 IP 地址。在更改用户所加入的虚拟网时，也不必重新改变设备的物理连接。虚拟网技术提供了动态组织工作环境的能力。

VLAN 简化了网络的物理结构，使网络管理、网络性能和网络安全提高到一个新的层次。有人说：“交换是虚拟网的基础，虚拟网是交换网的灵魂”，这句精练的语言正说明了虚拟网的重要性。

虚拟网技术是 OSI 第 2 层的技术，每个 VLAN 等效于一个广播域，广播信息仅发送到同一个 VLAN 的所有端口，虚拟网之间可隔离广播信息，如图 4-39 所示。与使用路由器分割一个网段（子网）一样，虚拟网也是一个独立的逻辑网络，每个 VLAN 都有唯一的子网号。因此，虚拟网之间通信也必须通过三层设备完成。

## 4.7.2　VLAN 的划分

划分 VLAN 是通过使用软件定义 VLAN 成员实现的，通常有多种不同的定义方法，以下

仅介绍 4 种目前常用的对虚拟局域网成员的定义方法。

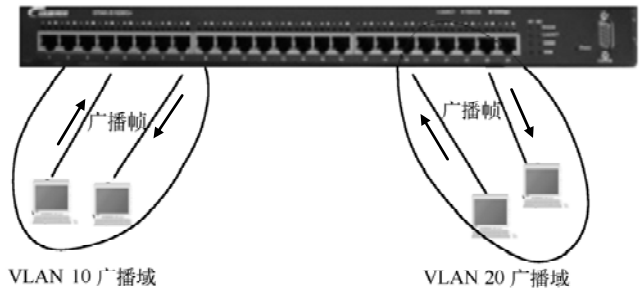



图 4-39　虚拟局域网

### 1．用交换机端口号定义虚拟局域网

许多早期的虚拟局域网都是根据局域网交换机的端口来定义虚拟局域网成员的。虚拟局域网从逻辑上把局域网交换机的端口分为不同的 VLAN，各 VLAN 相对独立，其结构如图 4-40 所示。图中局域网交换机端口 1、2 组成 VLAN 10；端口 3、4 组成 VLAN 20。

用局域网交换机端口划分 VLAN 成员是最通用的方法。但是，纯粹用端口定义 VLAN 时，不允许不同的虚拟局域网包含相同的物理网段或交换端口。例如，交换机 1 的 1 端口属于 VLAN 1 后，就不能再属于 VLAN 2。用端口定义 VLAN 的缺点是用户从一个端口移动到另一个端口时，网络管理者必须对 VLAN 成员进行重新配置。

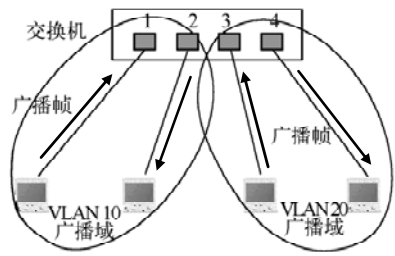



图 4-40　用端口号定义虚拟局域网

### 2．用 MAC 地址定义 VLAN

另一种定义 VLAN 的方法是用节点的 MAC 地址来定义 VLAN。这种方法的优点是：由于节点的 MAC 地址是与硬件相关的地址，所以用节点的 MAC 地址定义的 VLAN，允许节点移动到网络其他物理网段。由于节点的 MAC 地址不变，所以该节点将自动保持原来的 VLAN 成员地位。从这个角度看，基于 MAC 地址定义的 VLAN 可看做是基于用户的 VLAN。

用 MAC 地址定义 VLAN 的缺点是：要求所有用户在初始阶段必须配置到至少一个 VLAN 中，初始配置通过人工完成，随后就可以自动跟踪用户。但在大规模网络中，初始化时把上千个用户配置到某个 VLAN 中显然是很麻烦的。

### 3．用网络层地址定义 VLAN

另一种定义 VLAN 的方法是使用节点的网络层地址。例如，用 IP 地址来定义 VLAN。这种方法具有独特的优点：首先，它允许按照服务或应用的类型来组成 VLAN，这有利于组成基于服务或应用的 VLAN；其次，用户可以随意移动工作站而无须重新配置网络地址。对于 TCP/IP 用户特别有利。

与用 MAC 地址定义 VLAN 或用端口地址定义 VLAN 的方法相比，用网络层地址定义 VLAN 的缺点是性能比较差。检查网络层地址比检查 MAC 地址要花费更多的时间，因此用网络层地址定义 VLAN 的速度会比较慢。

4．用 IP 广播组定义 VLAN

这种虚拟局域网的建立是动态的，它代表了一组 IP 地址。虚拟局域网中由叫做代理的设备对虚拟局域网中的成员进行管理。当 IP 广播包要送达多个目的节点时，就动态建立虚拟局域网代理，这个代理和多个 IP 节点组成 IP 广播组 VLAN。网络用广播信息通知各 IP 站节点，表明网络中存在 IP 广播组，节点如果响应信息，就可以加入 IP 广播组，成为 VLAN 中的一员，与 VLAN 中的其他成员通信。IP 广播组中的所有节点属于同一个 VLAN，但它们只是特定时间段内特定 IP 广播组的成员。IP 广播组 VLAN 的动态特性有很高的灵活性，可以根据服务灵活组建，而且它可以跨越路由器形成与广域网的互联。

## 4.7.3　VLAN 内及 VLAN 间的通信

1．Port VLAN 成员端口间通信

Port VLAN 是基于端口的 VLAN，处于同一 VLAN 内的端口之间才能相互通信，可有效地屏蔽广播风暴，并提高网络的安全性。

实例：二层交换机上划分端口 3、23 属于 VLAN 1，端口 7、20 属于 VLAN 2。那么 VLAN 1 中的 PC1 和 PC2 之间可以通信，VLAN 2 中的 PC3 和 PC4 可以通信，但 PC1 和 PC3 之间不能通信，因为它们不在同一 VLAN 内，如图 4-41 所示。

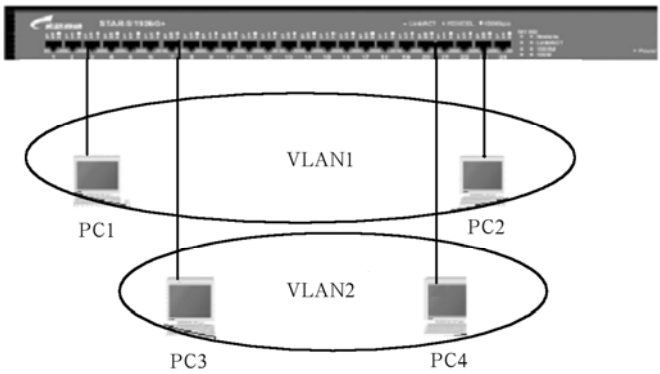



图 4-41　Port VLAN 的通信

2．Tag VLAN 成员端口间通信

802.1Q 协议使跨交换机的相同 VLAN 间的通信成为可能，它在以太网的帧头中加入 4 字节的 VLAN 标识（其中包含 2 字节的 802.1Q 帧标志，3 位优先级控制标志，1 位 CFI 通用标志及 12 位 VLAN 标识），当两交换机相连的端口被设置成 Trunk 模式时，该端口便能将以太网帧转变成 802.1Q 帧。交换机在从 Trunk 口转发数据前会在数据帧中打上一个 Tag 标签，在到达另一交换机后，根据此标签中的 VLAN 标识确定信息帧的转发。Tag VLAN 帧结构如图 4-42 所示。

Tag VLAN 用 VID 来标识不同的 VLAN，当数据帧通过交换机时，交换机根据帧中 Tag 头的 VID 信息来识别它们所在的 VLAN，这使得所有属于该 VLAN 的数据帧，都被限制在该逻辑 VLAN 中传播，而不受其他主机的影响，就像它们存在于单独的 VLAN 当中一样，如

图 4-43 所示。

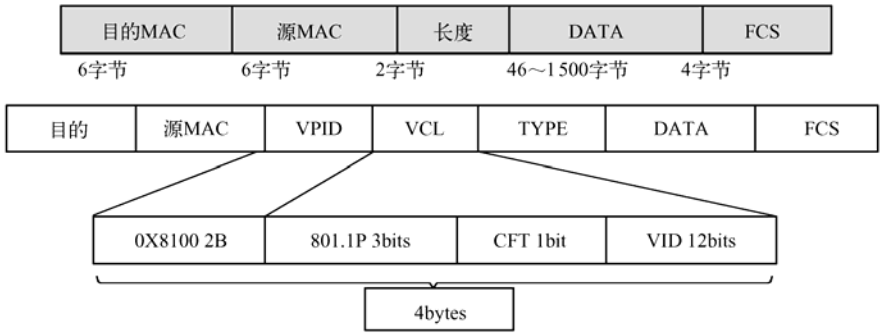



图 4-42　Tag VLAN 帧的结构

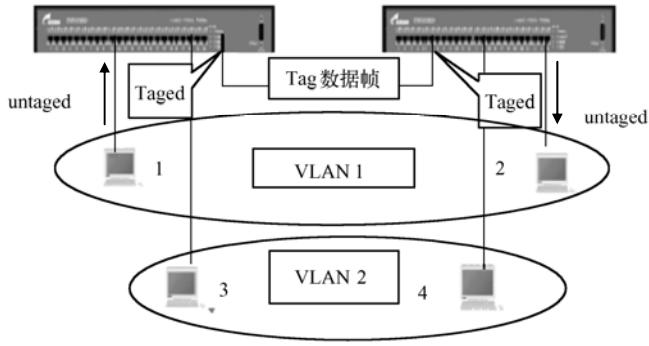



图 4-43　跨交换机的 VLAN 内的通信

### 3．VLAN 间的通信

在一般的二层交换机组成的网络中，VLAN 实现了网络流量的分割，不同的 VLAN 间是不能互相通信的。如果要实现 VLAN 间的通信必须借助三层网络设备。

（1）利用路由器实现 VLAN 间通信。

当每个交换机上只有一个 VLAN 时，路由器和交换机的接线方式如图 4-44 所示，只需在路由器上设置静态路由就可以实现三个 VLAN 间的通信。

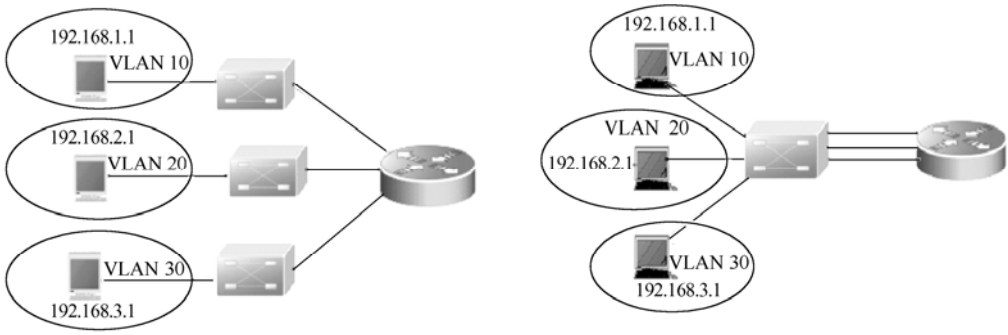



图 4-44　利用路由器实现 VLAN 间的通信

当每个交换机上有多个 VLAN 时，将路由器与交换机上的每个 VLAN 分别连接。前两种情况均须占用较多的路由器上的以太网端口。

不论交换机的 VLAN 有多少个，路由器与交换机都只用一条网线连接，这种方法占用路由器和交换机上的端口最少，但要求路由器与交换机都必须支持干路技术。

（2）利用三层交换机实现 VLAN 间通信。由于三层交换机有较多的端口，且具有一次路由多次快速转发的功能，故使用三层交换机可大大加快转发速度。在交换式以太网中多采用这种方法，如图 4-45 所示。

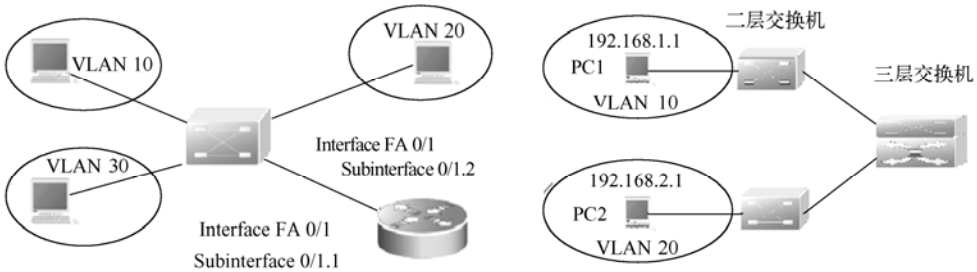



图 4-45　利用路由器的聚合功能或三层交换机实现 VLAN 间的通信

## 4.7.4　VLAN 的配置管理

Port VLAN 的配置功能及命令行格式如下所述。

（1）创建 VLAN 10，将它命名为 test。

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name test
Switch(config-vlan)# end
```

（2）把接口 0/10 加入 VLAN 10。

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
```

（3）将一组接口加入某一个 VLAN。

```
Switch(config)#interface range fastethernet 0/1-8, 0/15, 0/20
Switch(config-if-range)# switchport access vlan 20
```

**注意**：连续接口 0/1-8，不连续接口用逗号隔开，但一定要写明模块编号。

（4）把 F0/1 配成 Trunk 口。

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
```

```
Switch(config-if）# switchport mode trunk
```

（5）把端口 F0/20 配置为 Trunk 端口，但是不包含 VLAN 2。

```
Switch(config)# interface fastethernet 0/20
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

（6）验证配置信息。

```
Switch# show interfaces fastethernet 0/20 switchport
Switch# show vlan
```

# 练习 4

## 一、填空题

1．通过_____将单位办公室中的个人计算机和办公设备连接起来，以便实现_____和信息交换。

2．局域网是一个_____网络，目前最常用的局域网被称为_____网。

3．局域网的参考模型只对应于 OSI 参考模型的数据链路层与_____层，它将数据链路层划分为两个子层，分别被称为_____子层和 MAC 子层。

4．MAC 子层的主要功能是进行合理的信道分配，解决_____问题。LLC 子层的主要功能是建立、维持和释放_____。

5．以太网的最短帧长是_____位，最长帧中的用户数据可占_____位。

6．局域网中的硬件主要包括：_____、工作站、网络接口卡、_____、传输介质及介质连接部件，以及各种适配器等。

7．网卡最基本的功能包括：_____、_____和数据缓存。

8．根据网络软件的功能与作用，可分为网络_____软件和网络_____软件。

9．对等网也叫工作组网，是把联网的计算机组成一个工作组，且连入网内的计算机具有_____的地位，网络中没有_____。

10．在 C/S 模式中，发出资源请求的是_____；提供资源服务的是_____。

11．在一个冲突域中，如果使用Ⅱ类集线器，最多可以级连_____Hub，网络的最大直径为_____。

12．交换式局域网是指以数据链路层的_____或更小的数据单元（信元）为数据交换单位，以_____为基础构成的网络。

13．交换机连成的网络属于同一_____域；交换机上的每个接口都是一个_____域。

14．通过交换机上的配置端口（Console 口）对交换机进行管理。这种方法不占用交换机的_____，因此叫做_____管理。

15．虚拟局域网（VLAN）是以_____网络为基础，把网络上的用户用_____的方法分为若干个逻辑工作组或逻辑子网，每个逻辑工作组就是一个 VLAN。

## 二、选择题

（1）令牌环网是一个真正意义上的无冲突网，其原因是数据发送由（　　）。

A．各站点按顺序　　B．主控站控制　　C．令牌控制　　D．随意发送

（2）下面关于令牌总线网的论述中错误的是（　　）。

A．物理上采用总线结构　　B．逻辑上采用令牌控制方式

C．站点间有公平的访问权　　D．在任何情况下均不会发生冲突

（3）在组成局域网的可能设备中，资源的集中点是（　　）。

A．工作站　　B．服务器　　C．接口电路　　D．网络设备

（4）下面的描述中，不属于网络系统软件的是（　　）。

A．网络操作系统　　B．网络协议

C．通信软件　　D．管理信息系统

（5）不属于 C/S 模式主要特点的是（　　）。

A．属于二层结构的资源共享模式

B．所有的用户查询或命令处理都在工作站上完成

C．是一种平面形多层次的网状结构

D．应用被分为前端（客户端）和后端（服务器端）

（6）下面的描述中，不是 ATM 主要特点的是（　　）。

A．信元交换、面向连接　　B．综合各种业务服务

C．数据传输速率高　　D．仅是一种局域网技术

（7）以太网交换机的帧转发方式有（　　）等类型。

A．直接交换方式　　B．存储转发交换方式

C．改进的直接交换方式　　D．信元交换方式

（8）交换机连成的网络属于同一（　　）域。

A．冲突　　B．广播　　C．管理　　D．控制

（9）交换机的管理方式有（　　）。

A．带外管理　　B．带内管理　　C．自动管理　　D．手动管理

（10）对虚拟局域网成员的正确定义方法有（　　）。

A．用局域网交换机端口划分 VLAN　　B．用节点的 MAC 地址划分 VLAN

C．用网络层地址划分 VLAN　　D．用传输层的端口划分 VLAN

## 三、简答题

（1）简述 CSMA/CD 媒体访问控制方式的工作过程。

（2）试述 CS 结构和 BS 结构的区别。

（3）试述 ATM 网络的主要技术特点。

（4）试在交换机上创建 VLAN 10，并把接口 F0/2 加入 VLAN 10。

（5）你如何理解“交换是虚拟网的基础，虚拟网是交换网的灵魂”这句话？

# 第 5 章

# Internet 应用基础

Internet 是全球性的、开放的、最具有影响力的计算机互联网络，通常称为“因特网”、“互联网”等。作为全球范围的信息资源网，接入 Internet 的主机可以是信息资源及服务的提供者，也可以是信息资源及服务的使用者。分布在世界各地不同规模的计算机网络通过路由器，使用 TCP/IP 协议及其他有关协议互连起来形成大型网际网的 Internet，对全球的科学、文化、经济和社会的发展产生了巨大的影响。

## 5.1 Internet 基础知识

### 5.1.1 Internet 的起源和发展

Internet 诞生于 20 世纪 60 年代末，它的发展对推动整个世界、社会、科学、文化等领域的进步起到了不可估量的作用。

#### 1．Internet 的起源

1968 年，美国国防部的高级研究计划署提出了研制 ARPANET 的计划，目的是将多个大学、公司和研究所的多台计算机进行互联。1969 年，建成了具有 4 个节点的分组交换网络，这 4 个结点分布在 UCLA、UCSB、SRI 与 University Utah4 所大学。1971 年 2 月，建成了具有 15 个节点、23 台主机的网络并投入使用。ARPANET 是计算机网络诞生的标志。

1973 年，ARPANET 实现了与挪威和英格兰的计算机网络互连。从 1973—1974 年，TCP/IP 协议的体系结构和规范逐渐成形。

1982 年，ARPANET 又实现了与其他多个网络的互连，并开始全面由 NCP 协议转向 TCP/IP 协议。1983 年，ARPANET 分成两部分：一部分为军用网，称为 MILNET；另一部分为民用网，仍称 ARPANET。ARPANET 以 TCP/IP 协议作为标准协议，是早期的 Internet 主干网。TCP/IP 有一个非常重要的特点，就是开放性，即 TCP/IP 的规范和 Internet 的技术都是公开的。目的是使任何厂家生产的计算机都能相互通信，使 Internet 成为一个开放的系统。这正是后来 Internet 得到飞速发展的重要原因。

#### 2．Internet 的发展

Internet 的真正发展是从美国国家科学基金会 NSF（National Science Foundation）于 1986

年建成的 NSFNET 广域网开始的。NSFNET 对 Internet 的最大的贡献是使 Internet 向全社会开放，使得原来只有计算机科技人员参与的网络，吸引了很多其他研究人员和大学生参加，而且为 Internet 向社会普及打下了良好的基础。1988 年，NSFNET 连接的计算机数就猛增到 56 000 台。LNET 实现和 NSFNET 的连接之后，Internet 的名称被正式采用，NSFNET 也因此彻底取代了 ARPANET 而成为 Internet 的主干网。

由于 Internet 的开放性，它的应用很快进入文化、政治、经济、新闻、体育、娱乐、商业，以及服务行业并于 1992 年成立了 Internet 协会。20 世纪 90 年代美国的 IBM、MCI、MERIT3 家公司联合组建了一个 ANS 公司，建立了一个覆盖全美的 T3（44.746MB）主干网 ANSNET，并成为 Internet 的另一个主干网。1991 年年底，NFSNET 的全部主干网都与 ANS 的主干网 ANSNET 连通。与 NFSNET 不同的是，ANSNET 属 ANS 公司所有，而 NFSNET 则是由美国政府资助的。

ANSNET 的出现使 Internet 开始走向商业化的新进程，1995 年 4 月 30 日，NFSNET 正式宣布停止运作。随着商业机构的介入，出现了大量的 Internet 服务提供商（Internet Service Provider，ISP）和 Internet 内容提供商（Internet Content Provider，ICP），极大地丰富了 Internet 的服务和内容。世界各工业化国家，乃至一些发展中国家都纷纷实现与 Internet 的连接，使 Internet 迅速发展扩大成全球性的计算机互联网络，目前加入 Internet 的国家已超过 150 个。

Internet 在未来将成为社会信息基础设施的核心，将是计算、通信、娱乐、新闻媒体和电子商务等多种应用的共同平台。

### 3．Internet 在中国的发展

Internet 在中国的发展可以粗略地分成两个阶段：第一阶段是 1987—1993 年。这一阶段是 Internet 在中国的起步阶段。

1986 年，由北京计算机应用技术研究所（即当时的国家机械委计算机应用技术研究所）和德国卡尔斯鲁厄大学合作，启动了名为 CANET（Chinese Academic Network）的国际互联网项目。1987 年 9 月，在北京计算机应用技术研究所内正式建成我国第一个 Internet 电子邮件节点，通过拨号 X.25 线路，连通了 Internet 的电子邮件系统。随后，在国家科委的支持下，CANET 开始向我国的科研、学术、教育界提供 Internet 电子邮件服务。

1989 年，中国科学院高能物理所通过其国际合作伙伴——美国斯坦福加速器中心（SLAC）主机的转换，实现了国际电子邮件的转发。因而，国内科技教育工作者可以通过公用电话网或公用分组交换网，使用 Internet 的电子邮件服务。

1990 年 10 月，中国正式向国际互联网信息中心（InterNIC）登记注册了最高域名“CN”，从而开通了使用自己域名的 Internet 电子邮件。继 CANET 之后，国内其他一些大学和研究所也相继通过公用电话网或公用分组交换网开通了 Internet 电子邮件联结。

第二阶段是 1994 年至今。这一阶段是 Internet 在中国的发展阶段。我国实现了和 Internet 的 TCP/IP 连接，从而开始了 Internet 的全部功能服务，大型计算机网络项目正式启动，多个全国范围的计算机信息网络相继建立，Internet 在我国进入了飞速的发展时期。

1994 年 4 月 20 日，中关村地区教育与科研示范网络通过美国 Sprint 公司接入 Internet 的 64KB 国际专线开通，中国被国际上正式承认为有 Internet 的国家。1994 年 5 月，高能所的计算机正式进入了 Internet（后来发展为中国科学技术网络，CSTNET），1994 年 5 月 21 日完成

我国最高域名 CN 主服务器的设置，实现与 Internet 的 TCP/IP 连接，从而可向 NCFC（中国国家计算机与网络设施，始建于 1990 年）的各成员组织提供 Internet 的全功能服务。与此同时，以清华大学作为物理中心的中国教育与科研计算机网（CERNET）正式立项，并于 1994 年 6 月正式连通 Internet。1994 年 9 月，中国电信部门开始进入 Internet，中国公用计算机互联网（CHINANET）正式诞生。之后，原电子工业部系统的中国金桥信息网（CHINAGBN）也开通。1997 年，中国公用网络、中国科技网、中国教育和科研计算机网、中国金桥信息网实现了互联互通。随着中国 Internet 四大主力的崛起，以及政府部门制定“三金”工程，在中国，Internet 越来越成为人们科研工作甚至是日常生活中重要的一部分。

目前我国上网计算机数已超过 8 000 万台，另外受手机上网资费下调的影响，已有 27.3% 的网民使用手机上网，目前手机网民数已经有 4 430 万人。我国具备互联网上升期的典型特征，上网方式在逐步调整变化，日益多样化，更加顺应互联网发展需求。表 5-1 列出了七大主干网国际出口带宽数。从中可以看出 Internet 在中国发展之迅速。

表 5-1　七大主干网国际出口带宽数

| 主干网名称 | 国际出口带宽数（Mbps） |
|---|---|
| 中国公用计算机互联网（CHINANET） | 155 705 |
| 宽带中国（CHINA169）网 | 122 066 |
| 中国科技网（CSTNET） | 17 710 |
| 中国教育和科研计算机网（CERNET） | 4 796 |
| 中国移动网（CMNET） | 8 260 |
| 中国联通网（UNINET） | 3 807 |
| 中国国际经济贸易网（CIETNET） | 2 |

## 5.1.2　Internet 的信息服务方式

Internet 是一个全球性的巨大的计算机网络体系，它把全球数以万计的计算机网络，数千万台主机连接起来，具有丰富的信息资源，提供各种各样的服务。随着 Internet 的高速发展，它所提供的服务方式在不断增加，应用领域也不断扩大，成为人们日常工作和生活中不可缺少的组成部分。Internet 提供的主要信息服务方式包括以下几种：

### 1．万维网（WWW）

万维网（World Wide Web）简称 WWW。WWW 采用客户机/服务器模式（C/S 模式），利用超文本（Hypertext）、超媒体（Hypermedia）等技术，把图像、文本、声音和视频等多媒体信息集成起来，使用户能在 Internet 上已经建立了 WWW 服务器的所有站点提供超文本资源文档，允许用户通过浏览器检索远程计算机上的文本、图形、声音以及视频文件。WWW 是当前 Internet 上最受欢迎、最为流行、最新的信息检索服务系统。

（1）超文本标记语言

超文本标记语言 HTML（Hyper Text Markup Language）是一种专门的编程语言。超文本即在文本中添加了超级链接，超文本在形式上仍然是 ASCII 文件。超链接是一个多媒体文档中存在着指向相关文档的指针，通常是一些文字、图片和图形，用户单击这些文字或图片时，

会跳转到其指定的位置。

HTML 文档通常称为网页，其扩展名为“html”或“htm”。HTML 文档分为静态 HTML 和动态 HTML。静态的 HTML 文档的内容是固定不变的，动态的 HTML 文档也称为交互式的网页。是采用 ASP、ASP.net、PHP、Cold Fusion、CGI 等程序动态生成的网页。采用动态网页技术的网站可以实现更多的功能，如用户注册、用户登录、在线调查、用户管理、订单管理等。

（2）浏览器

WWW 浏览器（Browse）是访问 Web 的客户端软件，它是一个安装在客户机上，用来显示指定文件的交互程序，允许用户从 WWW 上查看信息。浏览器把在互联网上找到的文本文档（和其他类型的文件）翻译成网页。浏览器是 Internet 用户与 Web 服务器进行通信的软件，也是展示 Internet 丰富多彩的内容的窗口。比较典型的浏览器软件有 Netscape 的 Navigator、NCSA 的 Mosaic、Microsoft 的 Explorer 等。

（3）统一资源定位器 URL

统一资源定位器 URL（Uniform Resource Locator,）是 Web 的基本工具之一，是 HTML 文件地址命名方法。URL 是 WWW 页的地址，Web 上每个文档都有一个唯一的 URL。浏览 WWW 时，只需在浏览器的地址栏输入 URL 地址，就可以找到相应的网页。URL 地址的格式为：

<传输协议>：//<主机的域名或 IP 地址>/<路径文件名>

其中，<传输协议>定义所要访问的资源类型，对某些资源的访问，需给出相应的服务器提供的端口号。对于采用默认端口提供服务的服务器，端口号可省略，否则，需要用户在 URL 中指明。常用的 Internet 传输协议和默认端口号如表 5-2 所示。路径是指服务器上某资源的存放路径。与端口一样，路径也可以省略。如果路径文件名缺省，大部分主机会提供一个默认的文件名，如 index.html、default.html 或 homepage.html 等。

例如：

http://news.sohu.com/1/0903/62/subject212846206.shtml

各部分信息意义如下：

“http”表示使用超文本传输协议 HTTP 查询信息；

“news.sohu.com”表示“sohu”网站新闻主机的域名；

“/1/0903/62/subject212846206.shtml”表示该文件资源在主机中的路径和文件名。

**表 5-2　协议名称及其默认端口号**

| 协　　议 | 协 议 名 称 | 默认端口号 |
|---|---|---|
| HTTP | 超文本传输协议 | 80 |
| SMTP | 简单邮件传输协议 | 25 |
| Telnet | 远程登录协议 | 23 |
| FTP | 文件传输协议 | 21 |
| Gopher | 信息查询系统协议 | 70 |
| DNS | 域名解析服务协议 | 53 |
| NIC | 域名服务协议 | 101 |

续表

| 协　　议 | 协 议 名 称 | 默认端口号 |
| --- | --- | --- |
| POP3 | 邮局协议-3 | 110 |
| Kerberos | 安全认证系统 | 88 |

### 2．电子邮件服务

电子邮件（Electronic Mail），简记为 E-mail，它是 Internet 上使用最频繁、应用范围最广的一种服务。电子邮件允许用户在 Internet 上的各主机间发送和接收消息，即利用 E-mail 可以实现邮件的接收和发送。

（1）E-mail 的地址格式

在要使用电子邮件服务之前，要申请一个电子邮箱（Mail Box）。电子邮箱是用户向邮件服务器申请注册的。与普通邮件一样，电子邮件也必须按地址发送。电子邮件地址标识邮箱在网络中的位置。电子邮件地址包括两部分：用户名和提供邮件服务的邮件服务器的主机名，中间用@隔开。典型格式为：

Username@Hostname 或：用户名@主机名。

例如：sky@sina.com。

电子邮件具有唯一性，也就是说，每个电子邮件地址只能对应一个用户。但是，一个用户却可以拥有多个电子邮件地址。

（2）电子邮件的相关协议

SMTP 协议（Simple Mail Transfer Protocol）：SMTP 被用来在互联网上传递电子邮件。TCP/IP 协议族中，提供了两个电子邮件传送协议：邮件传送协议 MTP（Mail Transfer Protocol）和简单邮件传送协议 SMTP（Simple Mail Transfer Protocol）。

在 Internet 中，电子邮件的传送是依靠 SMTP 进行的。SMTP 的主要任务是负责服务器之间的邮件传送。在邮件的传送过程中，需要使用 TCP 协议进行连接。发送端主机先将邮件发送到本地 SMTP 服务器上，该服务器与接收方的服务器建立可靠的 TCP 连接，建立了发送方主机到接收方邮件服务器之间的直接通道，从而保证了邮件传送的可靠性。

POP 的全称是 Post Office Protocol，即邮局协议，用于电子邮件的接收，它使用 TCP 的 110 端口，现在常用的是第三版，所以简称为 POP3。POP3 的主要任务是实现当用户计算机与邮件服务器连通时，将邮件服务器的电子邮箱中的邮件直接传送到用户的计算机上。

IMAP（Internet Message Access Protocol）协议：消息访问协议，是一种电子邮件消息排队服务，它对 POP3 的存储转发限制提供了重要的改进。是一个用于接收来自用户的电子邮件的标准协议。IMAP 的最新版本是 IMAP4，这个客户端/服务器端模式的协议可以通过用户的因特网服务器接收或者保留用户的电子邮件。

目前，大部分的邮件服务器都采用 SMTP 用于电子邮件的发送，同时使用 POP3 或者 IMAP 接收电子邮件。

### 3．文件传输服务

文件传输协议（File Transfer Protocol），简称 FTP。是 Internet 上一种使用广泛、高效、快速传输大量信息的方式。利用文件传输协议，可以实现在各种不同类型的计算机系统之间传输各类文件。

FTP 是 TCP/IP 协议集中的应用层协议，基于 TCP 传输而不是 UDP，FTP 建立的是一个可靠的连接。采用 FTP 协议可使 Internet 用户高效地从网上的 FTP 服务器下载大量信息的数据文件，将远程主机上的文件复制到自己的计算机上。以达到资源共享和传递信息的目的。由于 FTP 的使用使得 Internet 上出现大量为用户提供的下载服务。所以使用文件传输服务的，通常要求用户在 FTP 服务器上有注册账号。但是，在 Internet 上，许多 FTP 服务器提供匿名（anonymous）服务，允许用户登录时以 anonymous 为用户名，以自己的电子邮件地址作口令。出于安全考虑，大部分匿名服务器只允许匿名 FTP 用户下载文件，而不允许上传文件。

FTP 服务的主要功能为以下几个方面：

（1）提供软件下载的高速站点。

（2）Web 站点维护和更新。

（3）在不同类型计算机之间传输文件。与两台计算机所处的位置、连接的方式、是否使用相同的操作系统无关。

#### 4．远程登录（Telnet）

远程登录是 Telnet 最早提供的基本服务功能之一。Telnet 中的用户远程登录是指用户使用 Telnet 命令，使自己的计算机暂时成为远程计算机的一个仿真终端的过程。一旦用户成功地实现了远程登录，用户使用的计算机就可以像一台与对方计算机直接连接的本地终端一样进行工作。

Telnet 的基本功能就是远程访问，共享远程系统中的资源，下面是 Telnet 的几种应用。

（1）资源共享：当用户使用 Telnet 远程登录到一台远程计算机上时，就可以像在本地终端操作一样使用远程计算机。

（2）匿名登录：当本地计算机没有提供某些 Internet 信息服务客户软件时，用户就无法使用这些服务，但可以使用 Telnet，直接连接到服务器上，使用这些服务。

（3）指定端口号的远程登录：在 TCP/IP 传输层协议的传输地址中包含一个进程端口号，端口号指明了应用类型。当建立 Telnet 会话时，若是指定某一端口号，就可以直接进入端口号所标识的应用进程，访问该信息服务。

（4）解决计算机兼容问题：远程登录解决了多种类型的计算机之间进行通信的问题。例如，某公司的数据库软件只能在 SUN 公司的计算机上运行，但是软件销售人员需要使用其他厂商的计算机访问该数据库时，就可以借助远程登录软件来实现。

运行 Telnet 程序进行远程登录的方法之一是：直接输入命令：

```
Telnet<远程主机网络地址>
```

### 5.1.3　Internet 相关组织

为了保证 Internet 可靠、健康地运行，国际上先后成立了一些自愿承担管理职责的非营利的组织或机构，为使 Internet 获取最大效益，它们遵循自下至上的结构原则。

#### 1．国际互联网协会（ISOC）

ISOC（Internet Society）成立于 1992 年，是一个非政府的全球合作性国际组织，主要工

作是协调全球在 Internet 方面的合作，就有关 Internet 的发展、可用性和相关技术的发展组织活动。ISOC 的网址为 http://www.isoc.org。

ISOC 的宗旨是：积极推动 Internet 及相关的技术，发展和普及 Internet 的应用，同时促进全球不同政府、组织、行业和个人进行更有效的合作，充分合理地利用 Internet。

ISOC 采用会员制，会员来自全球不同国家各行各业的个人和团体。ISOC 由会员推选的监管委员会进行管理。ISOC 由许多遍及全球的地区性机构组成，这些分支机构都在本地运营，同时与 ISOC 的监管委员会进行沟通。中国互联网协会成立于 2001 年 5 月，由国内从事互联网行业的网络运营商、服务提供商、设备制造商、系统集成商以及科研、教育机构等 70 多家互联网从业者共同发起成立。

### 2．国际互联网名字与编号分配机构（ICANN）

ICANN（Internet Corporation for Assigned Names and Numbers）成立于 1998 年 10 月，本部设在洛杉矶。ICANN 目前负责全球许多重要的网络基础工作，如 IP 地址空间的分配（原来是由 IANA 负责），协议参数（Protocol parameters）的配置，域名系统（DNS）与根服务器系统（Root Server System）的管理。根据 ICANN 章程的规定，ICANN 为一家非营利性公司，将在保证国际参与的前提下，负责协调互联网技术参数以保证网络的通信畅通，对 IP 地址资源以及域名系统进行管理和协调，以及监督域名系统和服务器系统的运行。

### 3．Internet 网络信息中心（InterNIC）

Internet 网络信息中心（Internet Network Information Center，InterNIC），网址是 http://www.InterNIC.net。InterNIC 成立于 1993 年 4 月 1 日，InterNIC 由三部分组成：注册服务（rs.internic.net），目录和数据库服务（ds.internic.net），以及信息服务（is.internic.net）。InterNIC 只分配网络号。主机号的分配由系统管理员来负责。

### 4．中国互联网络信息中心（CNNIC）

中国互联网络信息中心（China Internet Network Information Center，CNNIC）是成立于 1997 年 6 月的非营利 Internet 管理与服务机构，行使中国国家互联网络信息中心的职责。中国科学院计算机网络信息中心承担 CNNIC 的运行和管理工作，CNNIC 在业务上接受信息产业部领导，在行政上接受中国科学院领导。由国内知名专家、各大互联网络单位代表组成的 CNNIC 工作委员会，对 CNNIC 的建设、运行和管理进行监督和评定。

CNNIC 的主要任务包括：

（1）注册服务：域名注册、IP 地址分配、自治系统号分配等。

（2）目录数据库服务。

（3）信息服务。

（4）互联网寻址技术研发。

（5）网站访客流量认证。

（6）认证培训。

（7）国际交流与政策调研。

# 5.2　Internet 地址和域名

为了实现 Internet 上连接的所有主机之间的通信，每台主机必须有一个地址，能唯一的标识 Internet 上每台计算机和用户的位置。Internet 地址有两种表示形式：IP 地址和域名。

## 5.2.1　IP 地址的组成及分类

Internet 是通过路由器将物理网络互连在一起的虚拟网络。网络中的每一个节点都有其唯一的物理地址。但它只能标识出单个的设备，而标识不出其所属的网络。针对这一问题，因特网采用 TCP/IP 协议集中的 IP 协议提供的全网统一的地址格式。给每一台主机（包括路由器或网关）分配一个 IP 地址，用来屏蔽物理网络地址的差异。

### 1．IP 地址的组成

IP 地址是由网络地址（网络 ID 或网络号）和主机地址（主机 ID 或主机号）两部分组成，其结构如图 5-1 所示。其中，网络地址的前几位为类别号，用来标识网络类别，网络地址用来标识一个逻辑网络，主机地址用来标识网络中的一台主机。一台 Internet 主机至少有一个 IP 地址，这个 IP 地址是全网唯一的。如果一台 Internet 主机有两个或多个 IP 地址，则该主机属于两个或多个逻辑网络。


图 5-1　IP 地址的结构

目前主流的 IPv4 协议采用的 IP 地址长度为 4 字节，即 32bit 的二进制数。例如：10101100 10101000 00000000 00011001。由于二进制不容易记忆，在书写时，通常用 4 段十进制数表示（称为点分形式）：每段由 0～255 的数字组成，段与段之间用小数点分隔。例如：172.168.0.25。

### 2．IP 地址的分类

为了适应不同规模的网络应用，IP 地址分为五类：A 类、B 类、C 类、D 类、E 类。其中 A、B、C 类地址称为基本的 Internet 地址。D 类和 E 类为次类地址，D 类被称为组播地址，E 类被称为保留地址。五类 IP 地址的结构如图 5-2 所示。

（1）A 类地址

A 类地址的第 1 字节的第 1 位表示网络类别，其值为“0”，余下的 7 位表示网络 ID。A 类地址的后 24 位表示主机 ID。根据网络地址和主机地址的位数，得知 A 类地址允许的网络数为 $2^7$ 共 128 个，每个网络包含的主机数为 $2^{24}$ 共 16 777 216 个，A 类地址的范围是 0.0.0.0～

127.255.255.255.

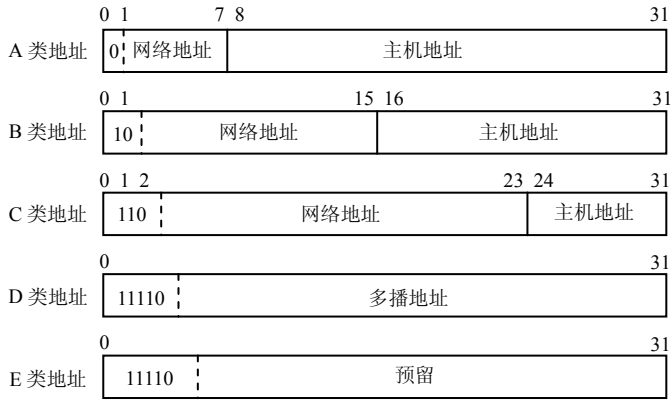



图 5-2　五类 IP 地址的结构

由于网络地址和主机地址全为“0”和全为“1”保留用于特殊用途，所以，A 类地址有效的网络数为 $2^7$–2=126 个，其范围是 1～126，每个网络包含的主机数应该为 $2^{24}$–2=16 777 214 个。因此，一台主机能使用的 A 类地址的有效范围是 1.0.0.1～ 126.255.255.254。A 类地址一般适用于有大量主机的大型网络。

（2）B 类地址

B 类地址的第 1 个字节的前两位表示网络类别，其值为“10”，余下的 6 位和第 2 个字节 8 位，共 14 位表示网络 ID。B 类地址的后共 16 位表示主机 ID。根据网络地址和主机地址的位数，得知 B 类地址有效地网络数为 $2^{14}$–2=16 382 个，每个网络包含的主机数应该为 $2^{16}$–2=65 534 个。因此，一台主机能使用的 B 类地址的有效范围是 128.0.0.1.～191.255.255.254。B 类地址一般适用于国际性的大公司和政府机构等。

（3）C 类地址

C 类地址的第 1 字节的前 3 位表示网络类别，其值为“110”，余下的 5 位和第 2、3 字节 16 位，共 21 位表示网络 ID。C 类地址的后 8 位表示主机 ID。根据网络地址和主机地址的位数， C 类地址有效地网络数为 $2^{21}$–2=2 097 150 个，每个网络包含的主机数应该为 $2^8$–2=254 个。因此，一台主机能使用的 C 类地址的有效范围是 192.0.1.1.～223.255.254.254。C 类地址一般适用于小公司和普通研究机构等。

（4）D 类地址

D 类地址的第 1 字节的前 4 位表示网络类别，其值为“1110”。D 类地址为多播地址，多播是指把数据同时发送给一组主机，只有那些已经登记可以接受多播地址的主机才能接收多播数据包。D 类地址的范围是 224.0.0.0～239.255.255.255。

（5）E 类地址

E 类地址的第 1 字节的前 5 位表示网络类别，其值为“11110”。E 类地址为预留地址，用于实验目的或将来使用，不能分配给主机使用。E 类地址的范围是 240.0.0.0～247.255.255.255。

使用点分十进制很容易识别 IP 地址所属的类别。根据对应的字段数值，可知“16.1.20.4”是 A 类地址、“136.22.10.5”是 B 类地址、“200.16.46.18”是 C 类地址。

IP 地址中的网络地址是由 Internet 网络信息中心 NIC（Network Information Center）来统

一分配的，主机地址由申请的组织自己来分配和管理，每个网点组成一个自治系统，负责自己内部网络的拓扑结构、地址建立及刷新等。

### 3．特殊的 IP 地址

（1）IP 地址的分配和使用规则

① 同一网络内的所有主机必须分配相同的网络地址和不同的主机地址；

② 不同网络内的主机必须分配不相同的网络地址，可以分配相同的主机地址；

③ 仅使用 IP 地址不能区分网络地址和主机地址，必须和网络掩码一起使用。

随着 Internet 的发展，可分配的 IP 地址越来越少，一般来说不是每台主机都能申请到合法的 IP 地址。为了解决这个问题，可以使用内部 IP 地址。有 3 种内部 IP 地址被预留并可供内部网使用：

A 类网络：10.0.0.0～10.255.255.255

B 类网络：172.16.0.0～172.31.255.255

C 类网络：192.168.0.0～192.168.255.255

（2）几种特殊的 IP 地址

① 直接广播地址。将主机地址各位全为 1 的地址称为直接广播地址。当某台主机需要发送广播时，可以使用定向广播地址向该网络上的所有主机发送报文。

② 有限广播地址。将网络地址和主机地址的 32 个比特全为 1 的 IP 地址称为有限广播地址，即“255.255.255.255”。有时需要在本网内部广播，但又不知道本网络号时，可使用有限广播地址。

③ 网络地址。将 IP 地址中主机地址位全为 0 的 IP 地址称为本网络地址，它用于表示“本地网络”。例如：用“130.16.0.0”表示“130.16”B 类网络；“202.102.46.0”表示“202.102.46”C 类网络。

④ 本机地址。将 IP 地址中网络地址和主机地址全为“0”的地址称为本机地址。

⑤ 回送地址。将网络号为 127 的 IP 地址作为保留地址，常用于网络软件测试以及本地主机进程间通信，又称为“回送地址”。即任何程序一旦接收到使用了回送地址为目的地址的数据，则该程序将不再转发数据，立即将其回送给源地址。最常用的回送地址是 127.0.0.1。

IP 地址的分配不是任意的，所有的 IP 地址都由国际组织 NIC 负责统一分配，目前全世界共有 3 个这样的网络信息中心。InterNIC 负责美国及其他地区 IP 地址分配；ENIC 负责欧洲地区 IP 地址分配；APNIC 负责亚太地区 IP 地址分配。

### 4．IPv4 到 IPv6

从 20 世纪 90 年代起，IPv4 就面临着地址空间的耗尽问题。随着 ADSL、Modem 和第三代无线设备的广泛使用，用户希望与所有需要全球 IP 地址的设备相连。IETF 认识到解决这一问题的唯一办法就是设计一个新版 IP 来取代 IPv4。IPv6 被指定为下一代 IP 协议，IPv6 与 IPv4 的主要区别如下：

（1）地址结构的变化。IPv4 是 32 位的，而 IPv6 是 128 位的，取消了 IPv4 地址分类的概念，将地址分为 3 种编址方式：单一通信、任意通信和组播通信。

（2）灵活的报头。IPv6 的报头分为基本首部和扩展首部，用扩展首部代替了 IPv4 的可变长度选项字段。可以根据功能要求设置不同的操作。

（3）简化了协议。IPv6 取消了首部校验和字段，报文分段只在原站进行。

（4）流标记功能。IPv6 增加了一种新的服务质量功能，给用户要求特别处理的特殊信息量流的分组做标记。

（5）安全性。IPv6 定义中实现了协议认证、数据完整性、报文加密等扩展功能。

目前 IPv4 技术广泛应用于 Internet 上，如何迁移到 IPv6 是一个非常值得关注的问题。尽管 IPv6 系统是向后兼容的，但现有的 IPv4 系统却无法直接处理 IPv6 数据包。要确保 IPv4 过渡到 IPv6，必须解决迁移问题。目前的解决方案主要是基于 IPv4 和 IPv6 功能的双 IP 层方法。有兴趣的同学可以参考相关读物来了解更多的方案。

## 5.2.2 子网与子网掩码

基于对管理、性能和安全方面的考虑，人们常把较大的网络划分成多个较小的物理网络，并使用路由器或第三层交换机将它们连接起来，每个较小网络使用不同的网络编号，这样的小网络被称为子网（Subnet）。子网划分（Subnetting）技术可使一个拥有多个物理网络的单位，将所属的物理网络划分成若干个子网，对外仍然表现为一个网络。

### 1．划分子网的原因

（1）充分使用现有的地址资源

为了更有效地利用 IP 地址资源，管理员可以通过子网划分技术将可用地址分配给多个较小的网络。由于 A 类网和 B 类网的地址空间很大，因此，子网划分技术能充分利用这些 IP 地址的资源。

（2）划分管理职责

当一个网络被划分为多个子网后，每个子网的管理可由子网管理员负责，使网络更易于控制，有利于网络管理员对网络用户、资源和计算机的管理。

（3）提高网络性能

随着网络用户的增多、主机的增加，网络通信将变得十分拥挤，大量的数据和广播信息在网络上传输，将导致网络性能和效率下降。如果将一个大型的网络划分成若干个子网，通过路由器连接各个子网，路由器在各个子网间转发数据时会自动隔离广播信息，从而改善了网络性能。另外，使用路由器的隔离作用还可以将网络分为内外两个子网，并限制外部网络用户对内部网络的访问，提高了网络的安全性。

### 2．划分子网的方法

划分子网的方法是将主机标识部分划出一定的位数用做本网的各个子网，其余的主机标识作为相应子网的主机标识部分。划分给子网的位数根据实际情况而定。这样 IP 地址就由三部分组成，即网络号、子网号和主机号。其中，网络号可以确定一个站点，子网号可以确定一个物理子网，而主机号可以确定与子网相连的主机。因此，一个 IP 数据包的路由就涉及三部分：传送到站点、传送到子网、传送到主机。

子网的划分方法如图 5-3 所示。

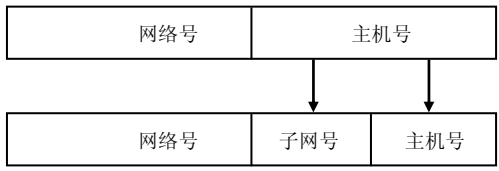



图 5-3　子网的划分方法

### 3．子网掩码

子网掩码（Subnet Mask）有两大功能：一是用来区分 IP 地址中的网络号和主机号，另一个功能就是将网络分割成多个子网。子网掩码是一个 32 位的二进制数，常用“点分十进制”表示。通过子网掩码，可区分一个 IP 地址中哪些位对应于网络地址（包括子网地址），哪些位对应于主机地址。

默认的子网掩码用在没有划分子网的 TCP/IP 网络。不同类型的网络使用的默认的子网掩码是不同的。将对应于 IP 地址中网络地址的所有位设置为“1”，对应于主机地址的所有位设置为“0”。将子网掩码和 IP 地址进行按位“与”操作，在“与”操作的结果中，非零字节即为网络号，而 IP 地址中剩下的字节就是主机号。标准的 A、B、C 类地址的默认子网掩码见表 5-3。

表 5-3　A、B、C 类地址的默认子网掩码

| 网络类型 | 子网掩码（二进制位表示） | 子网掩码（十进制表示） |
|---|---|---|
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

TCP/IP 对子网掩码和 IP 地址进行按位“与”的操作。按位“与”就是两个比特位之间进行逻辑“与”运算，即：1 and 1 = 1，1 and 0 = 0，0 and 0 = 0.经过按位与运算，可以将每个 IP 地址的网络地址取出，从而知道两个 IP 地址所对应的网络，如图 5-4 所示。

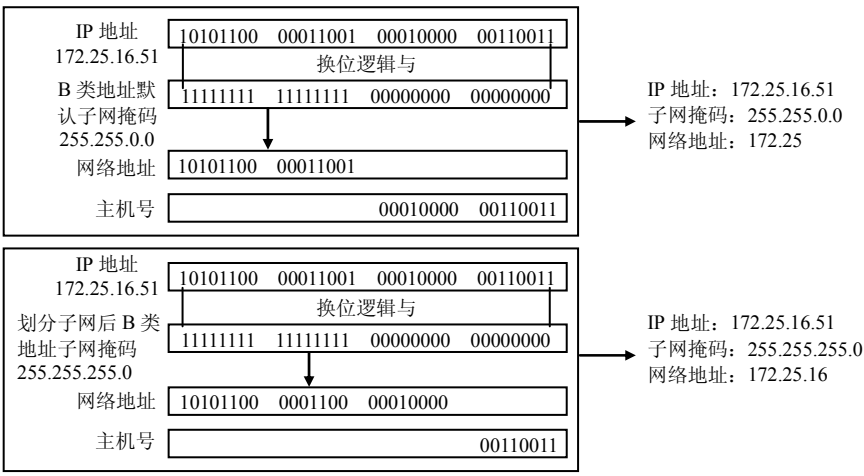



图 5-4　子网掩码的作用

可以得出结论：如果两个 IP 地址分别与同一个子网掩码进行按位“与”计算后得到相同

的结果，即表明这两个 IP 地址处于同一个子网中。

### 4．子网划分的规则

在 RFC 文档（Request For Comments 即“请求评议”包含了关于 Internet 的几乎所有重要的文字资料）中，RFC950 规定了子网划分的规范，其中对网络地址中的子网号作了如下的规定：

由于网络号全为“0”代表的是本网络，所以网络地址中的子网号也不能全为“0”，子网号全为“0”时，表示本子网网络。

由于网络号全为“1”表示的是广播地址，所以网络地址中的子网号也不能全为“1”，全为“1”的地址用于向子网广播。

RFC950 禁止使用子网网络号全为 0 和全为 1 的子网网络。在实际情况中，很多供应商主机的产品可以支持全为 0 和全为 1 的子网。对于可变长子网划分和 CIDR（Classless InterDomain Routing），属于现代网络技术，全为 1 和全为 0 的子网都可以使用。

### 5．子网划分实例

在划分子网之前，需要确定所需要的子网数和每个子网的最大主机数，有了这些信息后，就可以定义每个子网的子网掩码、网络地址（网络号+子网号）的范围和主机号的范围。

划分子网的步骤如下：

（1）确定需要多少子网号来唯一标识网络上的每一个子网。

（2）确定需要多少主机号来标识每个子网上的每台主机。

（3）定义一个符合网络要求的子网掩码。

（4）确定标识每一个子网的网络地址。

（5）确定每一个子网上所使用的主机地址的范围。

**例 1**：将一个 C 类网络 192.168.1.0，划分成两个子网，子网间用路由器连接。网络中有 100 台主机，请划分子网。

（1）确定子网掩码：从代表主机号的第 4 字节中取出两位，余下的 6 位，因 2^6=64，每个子网可容纳 62 个主机号（全为 0 和全为 1 的主机号不能分配给主机），又因 2^2=4，可划分成两个子网（00、01、10、11，而 00 和 11 不可用），所以，取出两位划分子网是可行的，子网掩码为 255.255.255.192。

（2）确定每个子网的网络地址：因为子网号的位数是 2，全为 0 和全为 1 的子网不能用，所以划分的两个子网的网络地址分别为 192.168.1.64 和 192.168.1.128，如图 5-5 所示。

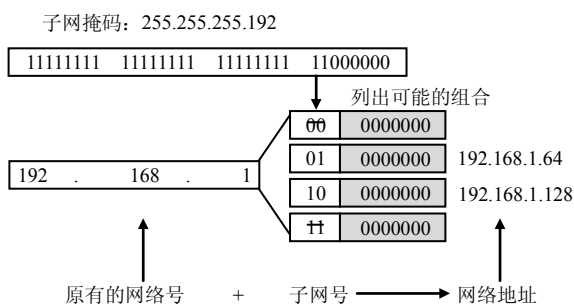



图 5-5　子网的网络地址

（3）确定每个子网的主机地址的范围，如图 5-6 所示。

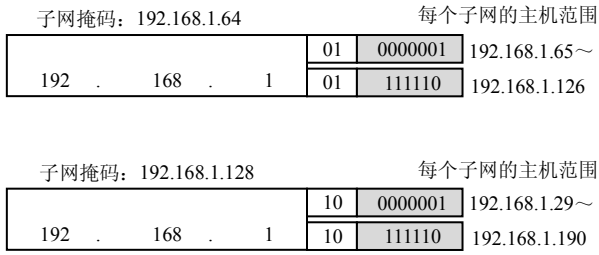



图 5-6　子网的主机地址的范围

（4）确定每个子网各台主机的地址配置，如图 5-7 所示。

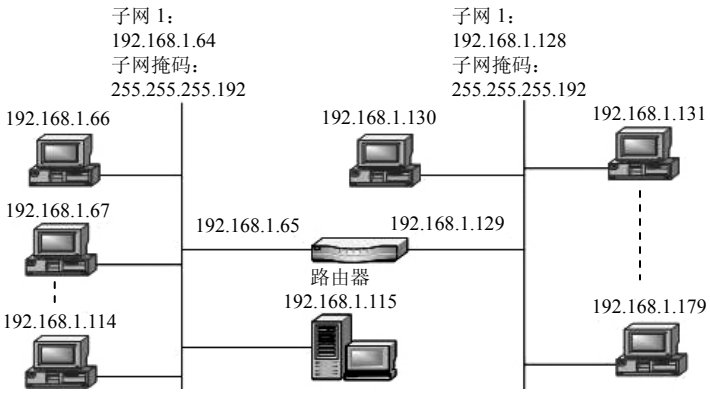



图 5-7　每个子网中每台主机的地址分配

**例 2**：现有一个公司需要创建内部的网络，该公司包括工程技术部、市场部、财务部和办公室四大部门，部门最大的计算机数目是 30 台。分配该公司使用的 C 类网络地址为 192.168.161.0，目前该网络广播数据过多，造成网络系统运行缓慢。请用子网划分的方法，解决上述问题。

解决具体步骤如下：

（1）设计思路

采用划分子网的方法，由于路由器隔离广播信息，可以控制各子网之间广播帧的传播。使得各个部门各自独立，能够提高各自的安全性能。

（2）设计要求

① 在公司的 4 个部门中，最大的计算机数目为 30 台，每个部门中有 1 台服务器要求 100Mbps 固定带宽，其他计算机要求 10Mbps 的带宽。

② 确定各部门使用的子网网络地址和子网掩码。

③ 确定可以分配给每个部门子网的主机 IP 地址范围。

④ 若采用交换式以太网，每个子网都使用一个交换式以太网，说明各主要设备的名称。

（3）设计方案

① 按照 RFC950 标准，子网号全为 1 和全为 0 的不能使用，则：

从主机号中取 3 位作子网号，得 2^3-2=6 个子网，符合 4 个子网的要求。主机号还余 5 位，则每个子网的允许的主机数为 2^5−2=30，所以子网掩码为 255.255.255.224。各子网的地

址和 IP 地址范围见表 5-4。

② 不按照 RFC950 标准，子网号全为 1 和全为 0 的全能使用，则：

从主机号中取 2 位作子网号，得 2^2=4 个子网，符合 4 个子网的要求。主机号还余 5 位，则每个子网的允许的主机数为 2^5−2=30，所以子网掩码为 255.255.255.192。各子网的地址和 IP 地址范围见表 5-5。

表 5-4　按照 RFC950 标准划分子网的结果

| 子网编号 | 子网地址 | 子网广播地址 | 子网主机的 IP 地址初值 | 子网主机的 IP 地址终值 |
|---|---|---|---|---|
| 1 | 192.168.1.32 | 192.168.1.63 | 192.168.1.33 | 192.168.1.62 |
| 2 | 192.168.1.64 | 192.168.1.95 | 192.168.1.65 | 192.168.1.94 |
| 3 | 192.168.1.96 | 192.168.1.127 | 192.168.1.97 | 192.168.1.126 |
| 4 | 192.168.1.128 | 192.168.1.159 | 192.168.1.129 | 192.168.1.158 |
| 5 | 192.168.1.160 | 192.168.1.191 | 192.168.1.161 | 192.168.1.190 |
| 6 | 192.168.1.192 | 192.168.1.223 | 192.168.1.193 | 192.168.1.222 |

表 5-5　不按照 RFC950 标准划分子网的结果

| 子网编号 | 子网地址 | 子网广播地址 | 子网主机的 IP 地址初值 | 子网主机的 IP 地址终值 |
|---|---|---|---|---|
| 1 | 192.168.1.0 | 192.168.1.63 | 192.168.1.1 | 192.168.1.62 |
| 2 | 192.168.1.64 | 192.168.1.127 | 192.168.1.65 | 192.168.1.126 |
| 3 | 192.168.1.128 | 192.168.1.191 | 192.168.1.129 | 192.168.1.190 |
| 4 | 192.168.1.192 | 192.168.1.255 | 192.168.1.193 | 192.168.1.254 |

③ 每个子网的主要设备为：一台 10/100Mbps 自适应式部门交换机；部门服务器使用 10/100Mbit/s 的 RJ-45 接口网卡；其他计算机可使用 10Mbps 的 RJ-45 接口网卡；采用 5 类 UTP 双绞线；RJ-45 水晶头若干。

根据以上分析，公司网络和子网结构如图 5-8 所示。

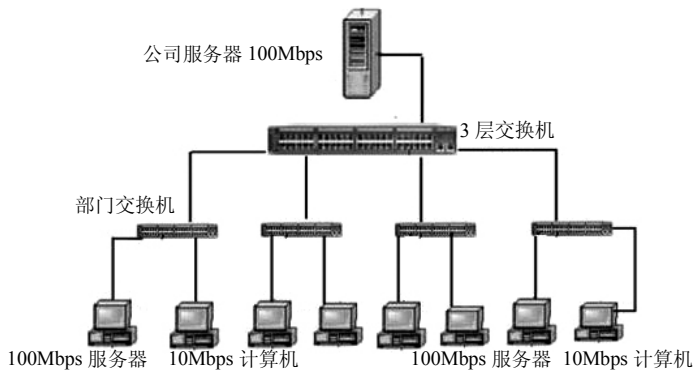



图 5-8　公司网络和子网结构

## 5.2.3　域名

在 TCP/IP 协议集中为 Internet 提供了统一的编址方式，即 IP 地址。使用 IP 地址人们就可以访问 Internet 中的主机，共享 Internet 中的资源。因为 IP 地址是以数字形式表示的，记忆

起来比较困难，于是人们提出用域名来表示主机的方法。这个工作由 DNS 域名系统来完成。

### 1．域名的概念

域名 DN（Domain Name）又称为主机标识符或主机名，可在 Internet 上唯一标识主机。域名由字符组成，名称具有一定含义且直观明了，容易记忆。例如：www.mit.edu 表示美国麻省理工学院 WWW 服务器，www.tsinghua.edu.cn 表示清华大学 WWW 服务器等。我们可以把域名地址和 IP 地址的关系比作一个人的姓名和身份证号码之间的关系，域名便于人们称呼和理解。

### 2．域名结构

Internet 的域名结构是由 TCP/IP 协议集的域名系统 DNS（Domain Name System）定义的。域名系统与 IP 地址的结构一样，采用的是典型的层次结构。一般情况下，一个完整而通用的域名由三部分组成，中间用圆点（.）隔开，可表示为：

…….三级域名.二级域名.顶级域名

由于在子域前面还有主机名，所以一台主机的域名可表示为：

主机名.三级域名.二级域名.顶级域名

完整的域名不超过 255 个字符，每一级域名都由英文字母和数字组成（不超过 63 个字符，并且不区分大小写字母），级别最低的在最左边，而级别最高的顶级域名写在最右边。互联网名称与数字地址分配机构 ICANN（Internet Corporation for Assigned Names and Numbers）是一个近年成立的、代替 NSI 公司的非营利机构，其主要职能包括管理互联网域名及地址系统。

（1）顶级域名

现在顶级域名大体上分为两大类：即组织模式和地理模式。组织模式是按组织管理的层次划分所产生的组织型域名，由 3 个字母组成，分为国际顶级域名 iTLD（只有 int）和通用顶级域名 gTLD。最早的通用顶级域名有 6 个，随着互联网上的用户急剧增加，在 2000 年 11 月，ICANN 又新增加了 7 个通用顶级域名，如表 5-6 所示。

表 5-6　Internet 顶级域名的代码和意义

| 域 名 代 码 | 意　义 |
|---|---|
| COM | 商业组织 |
| EDU | 教育机构 |
| GOV | 政府部门 |
| MIL | 军事部门 |
| NET | 网络支持中心 |
| ORG | 其他组织 |
| ARPA | 临时 ARPA（未用） |
| INT | 国际组织 |
| BIZ | 商业用途 |
| INFO | 任何企业和个人 |
| NAME | 个人 |
| PRO | 医生、律师、会计师等专业人员 |
| AERO | 航空运输业 |

续表

| 域 名 代 码 | 意　义 |
|---|---|
| COOP | 商业合作社 |
| MUSEUM | 博物馆 |

地理模式是指按国别地理区域划分所产生的地理型域名，也称国家顶级域名 nTLD，由两个字母组成，每个申请接入 Internet 的国家都以一个顶级域出现。例如：cn 代表中国，us 代表美国等。现在使用的国家顶级域名约有 200 个左右，如表 5-7 所示。

**表 5-7　部分国家或地区的顶级域名代码**

| 地 区 代 码 | 国家或地区 | 地 区 代 码 | 国家或地区 |
|---|---|---|---|
| CN | 中国 | FR | 法国 |
| AU | 澳大利亚 | SG | 新加坡 |
| RU | 俄罗斯 | DE | 德国 |
| JP | 日本 | TW | 中国台湾 |
| BR | 巴西 | HK | 中国香港 |
| KR | 韩国 | UK | 英国 |
| CA | 加拿大 | CH | 瑞士 |
| MO | 中国澳门 | IN | 印度 |
| EA | 南非 | SE | 瑞典 |

（2）第二级域名

网络信息中心 NIC 将顶级域的管理权授予指定的管理机构，各个管理机构再为它们所管理的域分配二级域名，将二级域名的管理权授予其下属的管理机构。如此层层细分，就形成了 Internet 的域名结构。

在我国，在二级域名 EDU 下申请注册三级域名由中国教育和科研（CERnet）计算机网络中心负责。中国教育和科研计算机网络中心将 EDU 划分为多个三级域，将三级域名分配给各个大学与教育机构。例如：edu 域下的 tsinghua 代表清华大学，并将 tsinghua 域的管理权授予清华大学网络中心管理。清华大学网络中心管理又将 tsinghua 域划分成多个四级域，分配给下属部门或主机。

Internet 主机域名的排列原则是低层的子域名在前面，而它们所属的高层域名在后面。Internet 主机域名的一般格式如图 5-9 所示。图为中国清华大学计算机系的主机域名的格式。

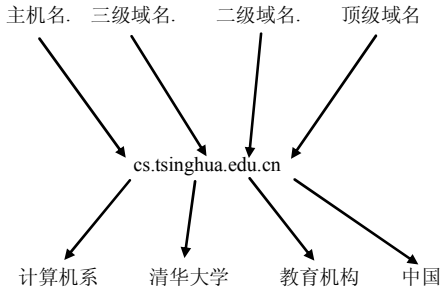



图 5-9　主机域名的格式

### 3．有关域名的几点说明：

（1）域名在 Internet 中必须是唯一的，当高级子域名相同时，低级子域名不允许重复。

（2）域名的字符通常为字母、数字和连字符，不区分大小写，但是各级子域名的长度必须小于 255。在 CNNIC 新的域名系统中，将同时为用户提供“.中国”、“.公司”和“.网络”结尾的纯中文域名注册服务，用户可以在这三种中文顶级域名下注册纯中文域名。其中注“.CN”的用户将自动获得“.中国”的中文域名，如注册“清华大学.CN”，将自动获得“清华大学.中国”。

（3）建议为主机确定域名时应尽量使用有意义的字符。

（4）一个域名对应一个 IP 地址，但是一个 IP 地址可对应多个域名。例如，一台计算机有一个 IP 地址，但是该主机既可以作为邮件服务器也可以作为 WWW 服务器，因而可以有多个域名。

（5）主机的 IP 地址和域名从使用的角度看没有区别。但是，如果使用的系统中没有域名服务器，则只能使用 IP 地址而不能使用域名。

### 4．域名系统

域名系统 DNS 是 Internet 对每台计算机命名方案的系统称呼。有了 DNS，当用户要和因特网上的一台主机相互通信时，只要使用域名，域名系统会自动将域名转换成 IP 地址，找到该计算机。

DNS 采用层次型名字管理机制，我们可以将它看成一个倒立的树，如图 5-10 所示。树的顶部为根节点。树根下的节点，我们称为域，每一个域还可以进一步划分为子域。根节点的下面是顶级域名，顶级域名的下面是二级域名，以此类推。域名树最下面是叶节点，即主机名。图中的二级域名 edu 的下面是三级域名为中国的高等院校的域名。其中，nankai 下有三台主机的名称：提供 FTP 服务的主机、提供 WWW 服务的主机和计算机系的主机。完整的域名由名字树中的一个节点到根节点路径上节点标识符的有序序列组成，其中节点标识符之间以“.”隔开。

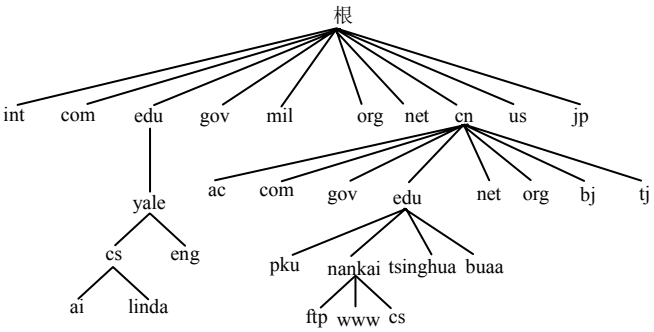



图 5-10　域名系统结构

由于数据在网络层必须根据 IP 地址进行传输，所以网络中还必须提供域名的解析，即将域名映射为相应的 IP 地址。DNS 系统的域名解析包括正向域名解析和反向域名解析两种类型。正向域名解析是指从域名地址映射为 IP 地址的过程；反向域名解析是指从 IP 地址映射为域名地址的过程。域名解析的工作是由域名服务系统的一组既相互独立又相互协作的 DNS

服务器自动完成的。域名服务器即一个服务器软件，运行在指定的主机上。一个域名服务器通常保存着它所管辖区域内的域名与 IP 地址对照表。

当一个应用进程需要将主机名解析成 IP 地址时，该应用进程就成为域名系统的一个客户，并将待解析的域名放在 DNS 请求报文中，以 UDP 数据报方式发给本地域名服务器。本地的域名服务器在查找到域名后，将对应的 IP 地址放在回答报文中返回。应用进程获得目的主机的 IP 地址后即可进行通信。若本地域名服务器不能回答该请求，则此域名服务器就暂成为 DNS 中的另一个客户，并向其他域名服务器发出查询请求，这种过程直到找到能够回答该请求的域名服务器为止。

域名服务器提供 3 种查询方式：即递归查询、迭代查询方式和反向查询方式。递归查询指一般客户机和服务器之间的查询过程，即当客户机向 DNS 服务器发出请求后，若 DNS 服务器本身不能解析，则会向另外的 DNS 服务器发出查询请求，得到结果后转交给客户机。迭代查询（反复查询）一般指 DNS 服务器之间的查询。反向查询指利用 IP 地址解析主机名的过程。

## 5.3 Internet 接入方式

随着 Internet 的迅速普及和发展，越来越多的单位和个人想使用因特网所提供的服务，因此选择一种合适的 Internet 接入方式，将自己的计算机接入 Internet，将变得非常重要。

Internet 服务提供者 ISP 是向社会提供公共 Internet 访问服务的公司和商业机构，其作用是帮助用户接入 Internet，并且向用户提供各种类型的信息服务，达到共享、访问资源的目的。我国的 ISP 有中国电信、中国联通、吉通、铁通、CERNET、CHINANET 等。

接入 Internet 的方式主要有 ISDN 接入、宽带接入、DDN 接入和无线接入等。无论使用哪种方式，用户计算机首先要通过某种通信线路连接到 ISP 的主机，再通过 ISP 的连接通道接入 Internet。

### 5.3.1 ISDN 接入

综合业务数字网 ISDN 分为窄带 ISDN（N-ISDN）和宽带 ISDN（B-ISDN）。N-ISDN 是 1970 年开发的网络技术，它的目的是以数字系统代替模拟电话系统，把语音、视频和数据业务在同一个网络上统一传输。

N-ISDN 即常说的“一线通”，是中国网通的 ISDN 业务名称，意为“一线多能，万事皆通”。通俗地说就是在一条普通电话线上，既能同时打两个电话，也能同时打电话和上网或进行可视电话通信的数字电话业务。ISDN 实现了从一个用户终端到另一个用户终端之间的转输全部数字化，包括用户线部分，以数字形式统一处理各种业务，使用户可以获得数字化的优异性能。如语音、数据、传真、可视图文、接入互联网等。

#### 1．ISDN 的特点

（1）上网速度更快，最低传输速率 64Kbps，最高可到 128Kbps。

（2）建立通话时间短、下载速度快、稳定可靠。

（3）线路使用率高。上网的同时可接、打电话或收发传真，实现一线两机。

（4）数字传输比模拟传输更不会受到静电和噪声的干扰，更少错误和重传，无须担心被人盗用、窃听。

（5）可支持局域网或多台 PC 单向接入互联网、城域网或广域网，费用比 DDN、Frame Relay、ATM 廉价，可作为这些链路的备份。

（6）开展电视会议、远程教学、远程医疗等安装可视电话，让远在天涯的亲友展现在眼前，或者作为远程监控。

**2．设备连接**

用户使用 ISDN 接入 Internet 时，需要安装一个一类 ISDN 终端（NT1），NT1 通过电话线路连接到电信局的 ISDN 交换机上。如图 5-11 所示。NT1 上可连接两类终端设备以及 ISDN 适配器。一类终端（TE1）是标准终端，如数字话机等；二类终端（TE2）是非 ISDN 标准终端，如模拟电话、Modem、计算机等；终端适配器（TA），完成适配功能，将非 ISDN 标准终端接入 ISDN 网络。

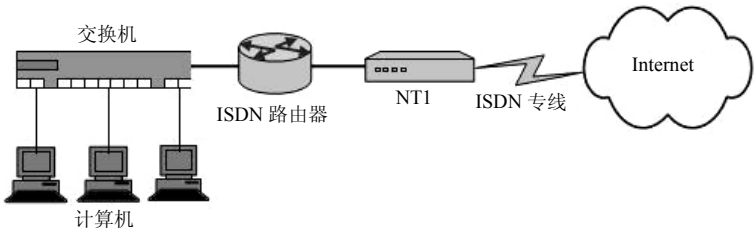



图 5-11　使用 ISDN 接入 Internet

ISDN 接入方式最主要的缺点还是受带宽限制，常用的对普通用户的基本速率接口（2B+D）最高仅能提供 128Kbps 的传输速率，只能适应低带宽的网络应用（如语音、可视电话等业务需求），但是无法满足网络日益增长的实时应用和多媒体应用对数据传输带宽的需求。

## 5.3.2　宽带接入方式

宽带（Broadband）是指在同一传输介质上，可利用不同的频道进行多重的传输，宽带接入就是利用各种高速率的接入技术连入互联网，来进行各种网上交互式活动，包括视频点播、网上广播、远程教学、视频会议等一系列在窄带条件下无法实现的互联网应用。通常人们把骨干网传输速率在 2.5GB 以上、接入网能够达到 1MB 的网络定义为宽带网。

宽带网建设分为 3 层：骨干网、城域网和社区接入网。骨干网相当于城市与城市之间的高速公路，城域网相当于城市市区内的道路，社区接入网解决的则是将道路从市区一直修到小区，抵达每户的家门口。

目前，实现宽带接入技术主要有 ADSL、Cable Modem 和光纤接入技术方式。

**1．ADSL 接入技术**

（1）ADSL 的概念

ADSL（Asymmetrical Digital Subscriber Line，非对称数字线路）是在普通电话线上传输

高速数字信号的技术。虽然传统的 Modem 也是使用电话线传输的。但只使用了 0～4kHz 的低频段，而电话线理论上有接近 2MHz 的带宽，ADSL 正是使用了 26kHz 以后的高频带才能提供高速的数据传输。经 ADSL 调制解调器编码后的信号通过电话线传到电信局后，通过 ADSL 交换机的信号识别分离器，如果是语音信号就传到电话交换机上，如果是数字信号就接入 Internet。

当电话线两端连接 ADSL 调制解调器时，在这段电话线上便产生了 3 个信息通道：一个速率为 1.5～9Mbps 的高速下行通道，用于用户下载信息；一个速率为 16Kbps～1Mbps 的中速双工通道，用于 ADSL 控制信号的传输和上行的信息；一个普通的电话服务通道；这 3 个通道可以同时工作。相对于 ISDN 技术，ADSL 即可以满足各种语音、数据业务的需求，提供了非常高的传输速度，因此被称作“超级一线通”。

一个 ADSL 调制解调器将多路下行通道中、双工通道中以及维护信道中的数据流组合成数据块，并在每一数据块中附加纠错代码，接收端则通过此纠错代码对在传输过程中产生的误码进行纠错。实验表明，此纠错编码技术完全可以达到 MPEG-2 和其他数字图像压缩方法在 Internet 上传输的要求。

目前 ADSL 中使用最为广泛的是数据的离散多音复用 DMT（Discrete Multitone）调制技术，DMT 技术可根据线路的情况调整在每个信道上所调制的比特数，以便更充分地利用线路。一般来说，子信道的信噪比越大，在该信道上调制的比特数越多。如果某个子信道的信噪比很差，则弃之不用。由于上网和打电话是分离的，所以上网时不占用电话信号，只需缴纳网费而不交电话费。

ISP 提供的接入服务主要有专线接入和虚拟拨号两种方式。专线方式用户有固定的 IP 地址，与局域网一样，打开计算机就可以上网，相对比较简单。比较常用的是虚拟拨号方式，目前最常用的是 PPPoE。PPPoE 方式是在标准的以太网协议和 PPP 协议之间加入一些小的更动，使用户可以在以太网上建立 PPP 的会话。对于 xDSL 调制解调器的要求是能够支持以太网网桥的应用。PPPoE 沿袭了人们习惯使用的拨号上网的方式，不要求对用户端的 ADSL 调制解调器进行复杂的设置，使用目前的标准网卡连接计算机和 ADSL 调制解调器，并且允许多台计算机同时共享 ADSL 线路。

（2）ADSL 接入技术

使用 ADSL 接入 Internet 需要在计算机上安装一块 10Mbps 或 10Mbps/100Mbps 自适应网卡，网卡通过网线连接到 ADSL 调制解调器上，ADSL 调制解调器和普通电话机通过电话线连接到信号分离器上，信号分离器最后通过电话线路连接到电信局的 ADSL 交换机上。连接方式如图 5-12 所示。

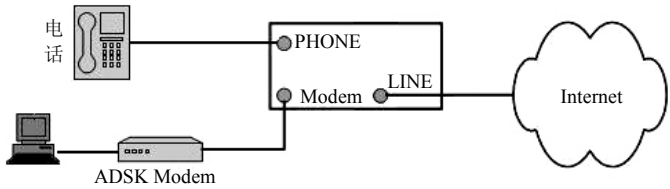



图 5-12　ADSL 接入 Internet

（3）ADSL 的特点

① 传输速率高：理论上，ADSL 的传输速率上行最高可达 640Kbps，下行最高可达 8Mbps。用户可以在互联网上自由冲浪，无须等待。

② 独享带宽安全可靠：与某些网络的共享网络带宽相比，ADSL 直接连接到电信宽带网的机房，用户独享带宽。ADSL 骨干网采用中国网通遍布全城全国的光纤传输，各节点采用 ATM 宽带交换机处理交换信息，独享带宽，信息传递快速可靠安全。

③ 上网打电话互不干扰，价格实惠：ADSL 数据信号和电话音频信号以频分复用原理调制于各自频段互不干扰。数据传输不通过电话交换机，无须支付上网通信费。

④ 安装快捷方便：在现有电话线上安装 ADSL，只需在用户端安装一台 ADSL Modem 和信号分离器，用户线路不用任何改动，极其方便。

### 2．Cable Modem 接入技术

Cable Modem（线缆调制解调器）是一种可以通过有线电视网络进行高速数据接入的设备。近年来，传统的有线电视网络陆续开始采用光纤同轴电缆混合传输结构。光缆是铺设到小区，然后通过光电转换节点，利用有线电视的树形同轴电缆网络连接到终端用户，作为宽带综合业务的接入平台。一般光纤干线采用星形拓扑，同轴电缆分配网采用树形结构，因此 Cable Modem 通常等同于 HFC 宽带接入技术。

（1）Cable Modem 的工作原理

Cable Modem 与以往的调制解调器在原理上都是将数据进行调制后变成模拟信号在电缆的一个频率范围内传输，接收时进行解调，将模拟信号转换为数字信号，输入计算机，其传输机理与普通调制解调器相同。但 Cable Modem 本身不单纯是调制解调器，它一般有两个接口，一个用来接有线电视端口，另一个与计算机相连，它集调制解调器、调谐器、加密解密设备、桥接器、网络接口卡、简单网络管理协议代理和以太网集线器的功能于一身，且通过 HFC 网的某个传输频带进行调制解调。普通调制解调器的传输介质在用户与交换机之间是独立的，即用户独享通信介质。Cable Modem 则属于共享介质系统，其他空闲频段仍然可用于有线电视信号的传输。

在使用 Cable Modem 传输数据时，利用的是现有的有线电缆中的某一个频道。可将整个电缆划分为 3 个宽带，分别用于 Cable Modem 数字信号的上传、数字信号的下载及电视节目模拟信号下载。一般同轴电缆的频道范围为 5～860MHz，数字信号上传为 5～42MHz，模拟信号下载为 50～550MHz，数字信号下载则是 550～860MHz。

通过 Cable Modem 系统，用户可在有线电视网络内实现国际互联网的访问、IP 电话、视频会议、视频点播、远程教育、网络游戏等功能。一个 Cable Modem 要在两个不同的方向上接收和发送数据。它把上行的数字信号转换成模拟射频信号，类似电视信号，在有线电视网上传送；在下行方向上，Cable Modem 把射频信号转换为数字信号，以便计算机处理。

（2）Cable Modem 的接入方式

HFC 网络宽带用户线接入方式，大致有两种方法：一种是多用户共享 Cable Modem 的以太网入户方式，可通过下连集线器支持最多台 PC 上网；PC 的 IP 地址，通过 DHCP 服务器动态获得。另一种是同轴电缆入户，用户独享 Cable Modem 的双向网络方式，用户可通过计算机以太网卡或 USB 口，连接到 Cable Modem；PC 的 IP 地址，可通过头端 DHCP 服务器动

态获得。

由于 Cable Modem 模式采用的是相对落后的总线形网络结构，这就意味着网络用户共同分享有限的带宽，因此会造成数据传输不够稳定，传输速率降低。例如，一个光节点覆盖 1 000 户，共享 40Mbps 的下行通道。如果有 20%的用户申请宽带接入，其中 20%的用户同时上网，则共有 40 个用户共享带宽，平均每户接入速率可以达到 1Mbps。实际上，可以通过减少光节点覆盖小区用户数或用扩充频道的方式来解决。

Cable Modem 接入 Internet 的示意图如图 5-13 所示。

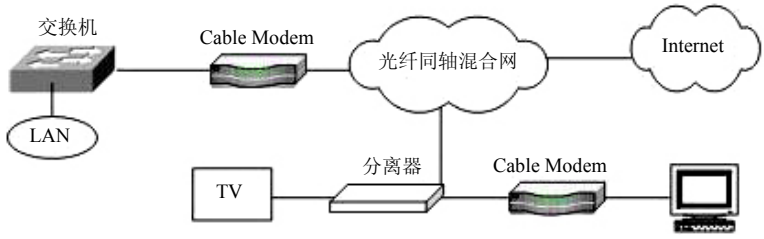



图 5-13　Cable Modem 接入 Internet

### 3．光纤接入技术

光纤由于其大容量、保密性好、不怕干扰和雷击、质量小等诸多优点，正在得到迅速发展和应用。主干网线路迅速光纤化，光纤在接入网络中的广泛应用也是一种必然趋势。光纤接入技术实际就是在接入网络中全部或部分采用光纤传输介质，构成光纤用户环路（或称光纤接入网 OAN），实现用户高性能宽带接入的一种方案。根据光网络单元所设置的位置，光纤接入网分为光纤到户（FTTH）、光纤到路边（FTTC）、光纤到大楼（FTTB）、光纤到办公室（FHHO）、光纤到楼层（FTTF）、光纤到小区（FTTZ）等类型。这几种类型都被统称为 FTTx 光纤接入方式。其中 FTTH 将是未来宽带接入网的发展趋势。

光纤接入的特点如下：

① 传输距离远：光纤连接距离可达 70km。

② 传输速度快：光纤接入能够提供 10Mbps、100Mbps、1 000Mbps 的高速带宽。

③ 损耗低：由于光纤介质的制造纯度极高，所以光纤的损耗极低，这样，在通信线中可以减少中继站的数量，提高了通信质量。

④ 抗扰能力强：因为光纤是非金属的介质材料，使用光纤作为传导介质，不受电磁干扰。

FTTx+LAN 接入方式利用 FTTx（光纤到小区或楼）+LAN（网线到户）的宽带接入方式实现“千兆到小区、百兆到大楼、十兆到桌面”的宽带接入方案，小区内的交换机和局端交换机以光纤相连，小区内采用综合布线，号称用户上网速率最高可达 10Mbps 或 100Mbps，但限于 ISP 提供的实际带宽有限或多用户共享后实际带宽的下降，其使用高峰期的速度可能达不到此速率。

FTTx+LAN 接入方式比较适合相对集中的住宅小区、智能大厦、现代写字楼使用，常又被俗称为“宽带局域网接入”。作为一种颇具发展潜力的宽带接入方式，FTTx+LAN 接入方式被各地 ISP 广为使用，而目前主流的无线宽带路由器大多都支持 FTTx+LAN 这种宽带接入方式，可利用 FTTx+LAN 接入方式实现无线宽带路由共享上网。

### 5.3.3　DDN 专线接入

数字数据网 DDN（Digital Data Network）是采用数字传输信道传输数据信号的通信网。数字数据网是比较流行的一种广域网技术。数字数据网能够提供点到点的连接，采用的通信介质可以是光纤、数字微波、卫星通信，用户接入时常常以铜介质、光纤和微波介质接入。

DDN 是由数字传输电路和相应的数字交叉连接复用设备组成。其中，数字传输电路主要以光缆传输为主，数字交叉连接复用设备对数字电路进行半固定交叉连接和子速率的复用。DDN 是利用数字信道来连续传输数据信号，不具备数据交换的功能，不同于通常的报文交换网和分组交换网。

数字数据网是以光纤为中继干线网络，组成 DDN 的基本单位是节点，节点间通过光纤连接，构成网状的拓扑结构，用户的终端设备通过数据终端单元（DTU）与就近的节点机相连。

DDN 传输的数据具有质量高、速度快、网络时延小等一系列的优点，特别适合于计算机主机之间、局域网之间、计算机主机与远程终端之间的大容量、多媒体、中高速通信的传输，DDN 可以说是我国的中高速信息国道。

DDN 专线是指运营商将 DDN 中的数据电路出租给用户，用户通过 DTU 直接进入运营商 DDN 网络的接入方式。

#### 1．DDN 的特点

（1）DDN 是透明传输网。DDN 将数字通信的规程和协议寄托在智能化程度的用户终端来完成，本身不受任何规程的约束，是一种面向各类数据用户的公用通信网，它可以看成是一个大型的中继开放系统，是全透明网。

（2）采用点对点或点对多点的专用数据线路，特别适用于业务量大、实时性强的用户。

（3）DDN 传输速率高，网络时延小。DDN 用户数据信息是根据事先的协议，在固定通道带宽和预先约定速率的情况下，按时隙通道准确地将数据信息送到目的地，无须目的端对信息的重组，因此减少了时延。另外，DDN 数据传输通道采用了时分复用技术，可以直接传送高速数据信号。

（4）DDN 可提供灵活的连接方式。DDN 可以支持数据、语音、图像传输等多种业务，它不仅可以和客户终端设备进行连接，而且可以和用户网络进行连接，为用户网络互连提供灵活的组网环境。

（5）网管中心能以图形化的方式对网络设备进行集中监控，电路的连接、测试、告警、路由迂回均由计算机自动完成，使网络管理智能化，减少不必要的人为错误。

（6）保密性高。花费较为昂贵，一般用于金融、无线移动通信网、气象、公安、铁路、医院、证券、银行等行业，特别是保密性要求高的行业。

#### 2．DDN 专线接入

DDN 专线需要铺设专用线路从用户端进入主干网络，用户端还需要专用的接入设备和路由器，DDN 专线接入如图 5-14 所示。

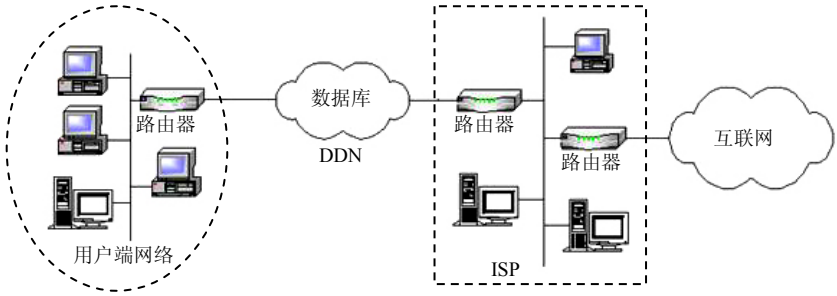



图 5-14　DDN 专线接入

### 5.3.4　无线接入

随着 Internet 以及无线通信技术的迅速普及，使用手机、移动计算机等随时随地上网已成为移动用户迫切的需求，随之而来的是各种使用无线通信线路上网技术的出现。

**1．无线接入的概念**

无线接入是指在终端用户和交换端局域网间的接入，全部或部分采用无线传输方式，为用户提供固定或移动接入服务的技术。无线接入技术与有线接入技术的一个重要区别在于可以向用户提供移动接入业务。作为有线接入网的有效补充，它有系统容量大，语音质量与有线一样，覆盖范围广，系统规划简单，扩容方便，可加密或用 CDMA 增强保密性等技术特点，可解决边远地区、难以架线地区的信息传输问题，是当前发展最快的接入网之一。

无线接入系统主要由用户无线终端（SRT）、无线基站（RBS）、无线接入交换控制器以及与固定网的接口网络等部分组成。其基站覆盖范围分为三类：大区制 5～50km，小区制 0.5～5km，微区制 50～500m。

**2．无线接入技术的类型**

无线接入技术主要有蜂窝技术、数字无绳技术、点对点微波技术、卫星技术、蓝牙技术等类型。下面介绍几种常见的无线接入技术。

（1）GSM 接入技术

GSM 技术是目前个人移动通信使用最广泛的技术，使用的是窄带 TDMA，允许在一个射频（即“蜂窝”）同时进行 8 组通话。

GSM 数字网具有较强的保密性和抗干扰性、音质清晰、通话稳定，并具备容量大，频率资源利用率高、接口开放、功能强大等优点。

GSM 网络手机用户可以通过无线应用协议 WAP（Wireless Application Protocol）上网。

目前，中国移动、中国联通各拥有一个 GSM 网，GSM 手机用户总数在 1.4 亿以上，为世界最大的移动通信网络。

（2）CDMA 接入技术

CDMA 即 Code-Division Multiple access 的缩写，译为“码分多址分组数据传输技术”，被称为第 2.5GB 移动通信技术。与 GSM 一样，也是属于一种比较成熟的无线通信技术。CDMA 是利用扩频技术，将所想要传递的信息加入一个特定的信号后，在一个比原来信号还大的宽

带上传输开来。当基地接受到信号后，再将此特定信号删除还原成原来的信号。这样做的好处在于其隐秘性与安全性好。与 GSM 不同，CDMA 并不给每一个通话者分配一个确定的频率，而是让每一个频道使用所能提供的全部频谱。

CDMA 数字网具有以下几个优势：高效地频带利用率和更大的网络容量、简化网络规划、提高通话质量、增强保密性、提高覆盖特性、延长用户通话时间、软音量和“软”切换，另外 CDMA 手机语音清晰，接近有线电话，信号覆盖好，不易掉线。

（3）GPRS 接入技术

GPRS 是通用分组无线业务（General Packet Radio Service）的英文简称，相对原来 GSM 的拨号方式的电路交换数据传送方式，GPRS 是分组交换技术。从技术上来说，声音的传送（即通话）继续使用 GSM，而数据的传送便可使用 GPRS，因此，就把移动电话的应用提升到一个更高的层次。而且发展 GPRS 技术也十分“经济”，因为只需沿用现有的 GSM 网络来发展即可。GPRS 的用途十分广泛，包括通过手机发送及接收电子邮件，在互联网上浏览等。

目前我国 GPRS（中国移动）和 CDMA（中国联通）都可以实现上网功能。

（4）蓝牙技术

蓝牙技术，实际上是一种短距离无线电技术。利用蓝牙技术，能够有效地简化掌上电脑、笔记本电脑和手机等移动通信终端设备之间的通信，也能够成功地简化以上这些设备与 Internet 之间的通信，从而使这些现代通信设备与因特网之间的数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙技术使得一些轻易携带的移动通信设备和计算机设备，不必借助电缆就能联网，并且能够实现无线上互联网，其实际应用范围还可以拓展到各种家用电器产品、消费电子产品和汽车等信息家用电器，组成一个巨大的无线通信网络。蓝牙技术是一种能够实现语音和数据无线传输的开放性方案。

“蓝牙”产品采用的是跳频技术，能够抗信号衰落；采用快跳频和短分组技术，能够有效地减少同频干扰，提高通信的安全性；采用前向纠错编码技术，以便在远距离通信时减少随机噪声的干扰；采用 2.4GHz 的 ISM（即工业、科学、医学）频段，以省去申请专用许可证的麻烦；采用 FM 调制方式，使设备变得更为简单可靠；“蓝牙”技术产品一个跳频频率发送一个同步分组，每组一个分组占用一个时隙，也可以增至 5 个时隙；“蓝牙”技术支持一个异步数据通道，或者 3 个并发的同步语音通道，或者一个同时传送异步数据和同步语音的通道。“蓝牙”的每一个语音通道支持 64Kbps 的同步语音，异步通道支持的最大速率为 721Kbps、反向应答速率为 57.6Kbps 的非对称连接，或者 432.6Kbps 的对称连接。

“蓝牙”原是一位在 10 世纪统一丹麦的国王，他将当时的瑞典、芬兰与丹麦统一起来。用他的名字来命名这种新的技术标准，含有将四分五裂的局面统一起来的意思。蓝牙技术产品与因特网之间的通信，使得家庭和办公室的设备不需要电缆也能够实现互通互连，大大提高了办公和通信效率。因此，“蓝牙”技术成为目前无线网络通信中被广泛应用的技术。

蓝牙的标准是 IEEE 802.15，工作在 2.4GHz 频带，带宽为 1Mbps。不过现在带宽 4 Mbps 的 IP（红外线）端口的产品已经非常普遍，而且最近 16Mbps 的扩展也已经被批准。

# 练习 5

## 一、填空题

（1）万维网是 Internet 最新、最普遍、使用最简单、功能最丰富的一种信息服务，通常被称作_____，它是一种基于_____技术的交互式信息浏览检索工具。

（2）_____是 Internet 上使用得最普遍的一种邮件协议，目前使用的是它的第三个版本，即_____。

（3）IP 地址由 32 位二进制位组成，通常分成_____地址和_____地址两部分。

（4）FTP 采用了_____工作模式。FTP 在传输文件时，要在客户程序和服务进程之间建立两个 TCP 连接，它们分别是_____连接和_____连接。

（5）网络掩码的作用，是使计算机能够自动地从 IP 地址中分离出相应的_____。

（6）在 WWW 服务中，统一资源定位器 URL 由三部分组成，即_____主机名与文件名。

（7）常用的 IP 地址有 A、B、C 三类，128.11.3.31 是一个_____类 IP 地址，其网络号为_____，主机号为_____。

（8）Cable Modem 是一种_____介质的接入技术，通过_____实现数据业务和传统的 CATV 业务共存。

## 二、选择题

（1）Internet 起源于（　　）年。

A．1969　　B．1975　　C．1946　　D．1979

（2）为了能够在因特网上正确地通信，每台联网的计算机都分配了唯一的地址，该地址由纯数字并用小数点分隔开，它称为（　　）。

A．WWW 服务器地址　　B．TCP 地址

C．WWW 客户机地址　　D．IP 地址

（3）IP 地址 202.112.10.64 中标识网络号的是（　　）。

A．202.112.10　　B．112.10.64　　C．202.112　　D．202

（4）下列四项中，合法的 IP 地址是（　　）。

A．190.220.5　　B．206.53.3.78

C．206.53.312.76　　D．123，43，82，220

（5）Internet 域名中的类型“com”代表的单位性质是（　　）。

A．商业　　B．共福利　　C．公共图书馆　　D．通信

（6）下列四项中，不是因特网的顶级域名的是（　　）。

A．EDU　　B．GOV　　C．WWW　　D．CN

（7）下列四项中，合法的电子邮件地址是（　　）。

A．Wang-em.hxing.com.cn　　B．Em.hxing.com.cn-Wang

C．Em.hxing.com.cn@Wang　　D．Wang@Em.hxing.com.cn

（8）TCP/IP 的含义是（　　）。

A．局域网传输协议　　B．拨号入网传输协议
C．传输控制协议和网际协议　　D．OSI 协议集

（9）从 www.seu.edu.cn 可以看出，它是中国的一个（　　）站点。
A．商业机构　　B．教育研究　　C．军事部门　　D．政府部门

（10）WWW 的中文名称为（　　）。
A．电子商务　　B．万维网　　C．浏览器　　D．网页

（11）在网址 http://www.sohu.com 中，“http”表示（　　）。
A．域名　　B．超文本　　C．超文本传输协议　　D．超级链接

（12）用户要想在网上查询 WWW 信息，必须安装并运行一个被称为（　　）的软件。
A．万维网　　B．网络服务器　　C．搜索引擎　　D．浏览器

（13）Outlook Express 是（　　）。
A．浏览器　　B．阅读器　　C．邮件专用软件　　D．电子邮箱

（14）Internet 实现了分布在世界各地的各类网络的互联，其最基础、最核心的协议是（　　）。
A．TCP/IP　　B．FTP　　C．HTTP　　D．NetBEUI

（15）在计算机网络中，允许一个地点的用户与另一个地点的计算机上运行的应用程序进行交互对话，称为（　　）。
A．传送电子邮件　　B．电子数据交换
C．远程登录　　D．联机会议

（16）以下对 FTP 服务叙述正确的是（　　）。
A．FTP 只能传送文本文件　　B．FTP 只能传送二进制文件
C．FTP 不能传送非二进制文件　　D．以上述说都不正确

（17）下述哪个不属于浏览器（　　）。
A．Internet Explorer　B．Netscape　　C．Opera　　D．Outlook Express

（18）系统对 WWW 网页存储的默认格式是（　　）。
A．PPT　　B．HTML　　C．XML　　D．DOC

（19）随着无线通信技术的迅速发展，一种提供近似于光纤通信带宽的新型无线通信技术是（　　）。
A．MMDS　　B．LMDS　　C．WLAN　　D．VLAN

（20）Internet 上各种网络和各种不同计算机间相互通信的基础是（　　）协议。
A．IPX　　B．HTTP　　C．TCP / IP　　D．X.25

## 三、判断题

（1）Internet 其实就是一台提供特定服务的计算机。（　　）
（2）域名系统就是把 IP 地址转换成域名。（　　）
（3）在 URL 中不能有空格。（　　）
（4）浏览器只能用来浏览网页，不能通过浏览器使用 FTP 服务。（　　）
（5）电子邮件程序从邮件服务器中读取邮件时，需要使用简单邮件传输协议（SMTP）。（　　）

（6）物理地址是指安装在主机上的网卡的地址。（　　）

（7）Internet 是 Intranet 对企业内部信息系统的应用和延伸。（　　）

（8）在用户访问匿名 FTP 服务器时，一般不需要输入用户名与用户密码。（　　）

（9）计算机网络产生的基本条件是通信技术与计算机技术的结合。（　　）

（10）IP 地址中的 127.X.X.X 是回送地址，用于网络软件测试和本地机进间通信。（　　）

**四、简答题**

（1）Internet 的相关组织有哪些?

（2）什么是 IP 地址、域名和物理地址？说明它们之间的关系。

（3）Internet 的基本服务功能有哪些？

（4）什么是子网掩码？请说出它的作用。

（5）常见的顶级域名是怎样划分的？种类有哪些?

（6）Internet 的宽带接入方式常用的有哪些？它们的特点是什么？

（7）Internet 的无线接入方式常用的有哪些?它们的特点是什么?

（8）在 Internet 中，某计算机的 IP 地址为 11001010.01100000.00101100.01011000。如何用十进制数表示上述 IP 地址？该 IP 地址是属于 A 类、B 类、还是 C 类地址？写出该 IP 地址在没有划分子网时的子网掩码。写出该 IP 地址在没有划分子网时计算机的主机号和网络号。若将该 IP 地址划分为 4 个子网，写出子网掩码及各个子网的 IP 地址范围（分别按 RFC950 标准和不按 RFC950 标准进行划分）。

（9）某公司的网络拓扑如图 5-15 所示。其中路由器具有 ISDN 模块，公司网络通过 ISDN 连接到 ISP。

① 在应用服务器关机的情况下，公司员工能连接上 Internet 吗？简要说明。

② 在路由器和 ISDN 之间需要加入终端适配器（TA）吗？试说明在什么情况下需要加入 TA。

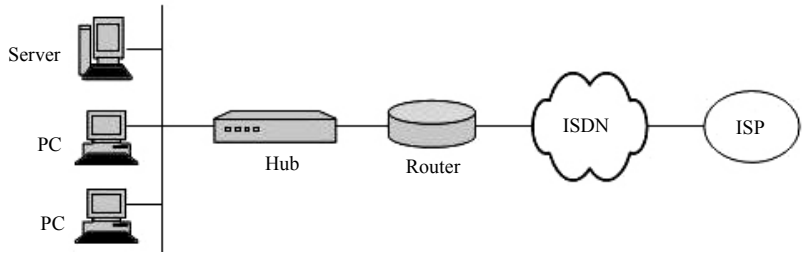



图 5-15　某公司的网络拓扑

（10）现有一个公司需要创建内部的网络，该公司包括工程技术部、市场部、财务部和办公室四大部门，部门最大的计算机数目有 50～60 台。分配该公司使用的 C 类网络地址为 192.168.166.0。试问：

① 如果将几个部门从网络上进行分开，如何划分子网？

② 确定各部门的网络 IP 地址和子网掩码，并写出分配给每个部门网络中的主机地址范围。

③ 若每个子网都使用交换式以太网，画出网络拓扑结构图。

# 第 6 章

# 网络操作系统

本章主要介绍网络操作系统的概念、分类、Windows Server 2003、活动目录服务、DHCP、DNS 服务等内容。

通过本章的学习，应达到如下学习目标：

（1）了解网络操作系统的概念、功能及分类；

（2）熟悉 Windows Server 2003 的特点及使用；

（3）熟悉 DHCP 服务的功能特点及其安装使用方法；

（4）熟悉 DNS 的功能特点及其基本使用方法。

## 6.1 网络操作系统概述

网络操作系统（Network Operating System，NOS）是在网络环境下，用户与网络资源之间的接口，用以实现对网络资源的管理和控制。对网络系统而言，所有网络功能几乎都是通过网络操作系统实现的，网络操作系统代表着整个网络的水平。随着计算机网络技术的不断发展，特别是计算机网络互联、异构网络互联技术及其应用的发展，网络操作系统朝着支持多种通信协议、多种网络传输协议、多种网络适配器的方向发展。

### 6.1.1 网络操作系统的特点

计算机网络系统是通过通信媒体将多个独立的计算机连接起来的系统，每个连接起来的计算机各自拥有独立的操作系统。网络操作系统是建立在网络服务器上，为网络用户提供使用网络系统资源的方法。在多个用户争用系统资源时，网络操作系统能进行资源调剂管理，网络操作系统还要协调和管理网络用户进程或程序与联机系统进行交互。

### 6.1.2 网络操作系统的功能

为实现有效的资源共享，首先要提供网络通信功能或支持协议，另外还要提供资源共享的途径及多个用户使用资源时解决冲突的方法。所以网络操作系统除了具备单机操作系统所需的功能，如内存管理、CPU 管理、输入/输出管理、文件管理等以外，还应具备如下一些网

络控制、管理和服务功能。

（1）提供高效可靠的网络通信功能。如对网络协议、网络硬件的支持。在 Windows 2003 操作系统中，就有对 TCP/IP、NetBEUI 等多种协议的支持，同时还提供了多种网络硬件的驱动程序。

（2）提供多项网络服务功能。如远程登录服务功能、文件传输服务功能、电子邮件服务功能、远程打印服务功能等。常用的 Telnet、FTP、E-mail 等都是该类服务功能的典型例子。

（3）提供网络资源管理、系统管理功能。如文件系统管理、网络服务进程的建立和管理、网络活动的监控和网络测试工具等。Windows 2003 中的事件查看器就具有对一些网络安全方面的问题进行监视的功能。

（4）提供对网络用户的管理。几乎所有的操作系统都提供了用户管理功能，用户管理功能所提供的用户访问控制机制有效地管理和控制了用户对网络资源的访问。用户必须提供合法的用户账号并在授权范围内访问网络资源就是用户管理的具体体现。

## 6.2 网络操作系统的分类

### 1．网络操作系统的类型

网络操作系统一般可以分为面向任务型与通用型两类。面向任务型网络操作系统是为某一种特殊网络应用而设计的；通用型网络操作系统能提供基本的网络服务功能，支持用户在各个领域应用的需求。

网络操作系统经历了从对等结构向非对等结构的演变过程。目前常用的网络操作系统均是非对等结构的网络操作系统。

非对等结构网络操作系统运行在服务器上。因为网络服务器集中管理网络资源与服务，所以网络服务器是局域网的逻辑中心。网络服务器上运行的网络操作系统的功能与性能，直接决定着网络服务功能的强弱以及系统的性能与安全性，它是网络操作系统的核心部分。 网络操作系统是网络设计与实施过程中要考虑的关键因素之一。比较典型的非对等网络操作系统有 UNIX/Linux、NetWare 以及 Windows NT、Windows Server 2003 等。

### 2．UNIX 操作系统

UNIX 最早是指由美国贝尔实验室发明的一种多用户、多任务的通用操作系统，经过长期的发展和完善，目前已成长为一种主流的操作系统技术和基于这种技术的产品家族。由于 UNIX 具有技术成熟、安全可靠、网络和数据库功能强、伸缩性以及开放性好等特点，可满足各行各业的实际需要，已经成为主要的工作站平台和重要的企业操作平台。它被广泛地运用在网络应用服务器、Web 服务器和数据库服务器等高端领域。

UNIX 目前发行的版本很多，如 Sun Microsystems 的 Solaris、IBM 的 AIX 等及其为兼容机而设计的 Xenix 和 System V/386 以及运行在 Macintosh 上的 AUX 等。由于其安全可靠，在我国的银行系统中被普遍使用。

### 3．Linux 操作系统

Linux 是开放的、可以在 PC 上运行、与 UNIX 相兼容的操作系统。Linux 的源代码被放

到 Internet 上自由传播，任人修改、充实和发展。十多年来，它已进入了成熟期，越来越多的人认识到它的价值，并被广泛应用到 Internet 服务器、图形工作站等各种领域。Linux 下有大量的免费应用软件，从系统工具、开发工具、网络应用，到休闲娱乐、游戏等。

Linux 作为一个置于共用许可证 GPL（General Public License）保护下的自由软件，任何人都可以免费从网站上下载。目前 Linux 的发行版本种类很多，最主要的几个发行版本为 Red Hat Linux、S.u.S.e Linux 等，国内也有人搞了自己的发行版本，如联想公司的幸福 Linux 以及冲浪平台的 Xteam Linux。

### 4．NetWare 操作系统

Novell 公司的 NetWare 网络操作系统是目前应用较广泛的局域网操作系统之一。

NetWare 推出时间比较早，经过多年的发展，可以提供非常稳定的运行性能。在一个 NetWare 网络中允许有多个服务器。NetWare 的主要优点如下：

（1）强大的文件及打印服务能力；

（2）兼容性及系统容错能力；

（3）比较完备的安全措施。

NetWare 主要的不足之处是工作站资源无法直接共享，安装及管理维护较为复杂，多用户需同时获取文件及数据时会导致网络效率降低，以及服务器的运算功能没有得到充分的发挥等。

### 5．Windows 操作系统

Microsoft 公司在 1993 年才推出第一代网络操作系统产品 Windows NT 3.1，随着 Windows NT 3.1 的问世，Microsoft 正式加入网络操作系统的市场角逐。时至今日，微软公司先后对其 Windows 网络操作系统不断进行改进，陆续推出 Windows NT 3.5、Windows NT 4.0、Windows Server 2000 家族，以及目前常用的 Windows Server 2003。Windows 系列网络操作系统的主要特点有以下几个方面：

（1）可靠性。用可靠性衡量一个网络操作系统不是一朝一夕的事，无论 Microsoft 在软件界的地位有多高，它新推出的 Windows NT（2000/2003）在未经历相当时间的检验之前，系统的可靠性、稳定性还是未知数，慎重的客户也不会盲目地一下子拥向 Windows NT，所以现在比较慎重的用户在一些重要场合还是坚持使用 UNIX。

（2）新概念和新技术。因为 Windows NT 是较新设计的网络操作系统，它自然而然就会采用最新的概念和最新的技术。以前的网络操作系统在设计时根本不会考虑到的因素，Windows NT 的设计者都考虑到了，这绝不是说别的系统不够先进或没有远见，只是受当时的技术发展因素所限，不可能预见到。

（3）友好的界面。Windows NT 具有友好的界面。统一的界面风格是 Windows 系列开拓市场的强有力的武器。简单的操作使用户免于记忆繁杂的命令，一上手就可以使用，更重要的是，Windows NT 提供的功能以及开发工具绝不逊色于任何其他系统。

（4）丰富的配套应用。Microsoft 公司在软件界有着特殊的地位，一方面它是平台提供商，另一方面它也是应用提供商。这样的双重身份使得 Microsoft 的产品具有一些特别之处。对于网络操作系统产品而言，因为 Microsoft 本身就是应用提供商，所以在其上的应用服务就不会匮乏，而且，是出自同一公司之手，因而应用和平台的结合应当是优秀的。应用可以充分利

用 Microsoft 的平台优势，平台也能充分支持基于它开发的各种应用。此外，新开发的 Windows 2000/2003 的 VLM 将提供大内存寻址能力和动态目录服务，弥补了 Microsoft 在这方面的不足。Microsoft 的“零管理”也将大大降低系统的管理成本。

正是由于上述优越的性能，使得 Microsoft 的 Windows 网络操作系统系列产品后来居上，在当今的网络操作系统市场中占有举足轻重的地位。

## 6.3 Windows Server 2003 简介

Windows Server 2003 是微软（Microsoft）公司推出的新一代的强大、安全、易用的网络操作系统，它不仅继承了 Windows Server 2000 的安全性、可管理性与可靠性，而且还融合了 Windows XP 的易用性、人性化、智能化特点，并在此基础上提供了更丰富的功能和更稳定的内核，非常适合搭建中小型网络中的各种网络服务，尤其适合那些没有经过专业培训的非专业管理人员使用。

### 6.3.1 Windows Server 2003 的基本特点

与以前的 Windows NT 和 Windows 2000 相比，Windows Server 2003 在程序运行的稳定性、程序的兼容性及操作系统的易学易用性上，都达到了一个崭新的高度。智能化的人机交互，随处可见的操作向导，稳定的程序运行平台以及无所不在的帮助系统，都可以让用户在轻松的环境中，完成对系统的配置、优化以及管理工作。

#### 1．Windows Server 2003 标准版

Windows Server 2003 标准版是一个可靠的网络操作系统，可迅速方便地提供企业解决方案。这种灵活的服务器是小型企业和部门应用的理想选择。其特性主要有：

① 支持文件和打印机共享；
② 提供安全的 Internet 连接；
③ 允许集中化的桌面应用程序部署。

#### 2．Windows Server 2003 企业版

Windows Server 2003 企业版是为满足各种规模的企业应用而设计的。它是各种应用程序、Web 服务和基础结构的理想平台，它提供了高度的可靠性、高性能和出色的商业价值。其特性主要有：

① 一种全功能的服务器操作系统，支持多达 8 个处理器；
② 提供企业级功能，支持高达 32GB 内存；
③ 可用于基于 Intel Itanium 系列的计算机。

#### 3．Windows Server 2003 Datacenter 版

Windows Server 2003 Datacenter 版是为运行企业和任务所倚重的应用程序而设计的，这些应用程序需要最强的可伸缩性和可用性。其特性主要有：

① 是 Microsoft 迄今为止开发的功能最强大的服务器操作系统；

② 支持高达 32 路的 SMP 和 64GB 的 RAM；

③ 提供 8 节点群集和负载平衡服务是它的标准功能。

#### 4．Windows Server 2003 Web 版

Windows 操作系统系列中的新产品，Windows Server 2003 Web 版用于 Web 服务和托管。其特性主要有：

① 用于生成和承载 Web 应用程序、Web 页面以及 XML Web 服务，其主要目的是作为 IIS6.0 Web 服务器使用；

② 提供一个快速开发和部署 XML Web 服务和应用程序的平台，这些服务和应用程序使用 ASP.NET 技术，该技术是.NET 框架的关键部分。

### 6.3.2　Windows Server 2003 的文件系统

硬盘文件系统是文件存储的基础。在所有的计算机系统中，都存在一个相应的文件系统，它规定了计算机对文件和文件夹进行操作处理的各种标准和机制。因此，用户对所有的文件和文件夹的操作都是通过文件系统来完成的。其中 NTFS、FAT 和 FAT32 都是文件系统的类型，它们也都是 Windows Server 2003 支持的文件系统。

#### 1．FAT 文件系统

FAT 文件系统最初是用于小型磁盘和简单文件结构的简单文件系统，它得名于它的组织方法：放置在卷起始位置的文件分配表。为确保正确装卸启动系统所必需的文件，文件分配表和根文件夹必须存放在固定的位置。

采用 FAT 文件系统格式化的卷以簇的形式进行分配。默认的簇大小由卷的大小决定。对于 FAT 文件系统，簇数目必须用 16 位的二进制数表示，并且是 2 的乘方，默认的簇大小如表 6-1 所示。通过使用命令行提示符下的 format 程序，用户可以指定簇的大小。不过，用户所指定的簇的大小必须大于表中所给出的大小。由于额外开销的原因，在大于 511MB 的卷中不推荐使用 FAT 文件系统。

表 6-1　FAT 文件系统默认的簇大小

| 分区大小（字节） | 扇区数/每簇 | 簇大小（字节） |
|---|---|---|
| 0～32MB | 1 | 521KB |
| 33～64MB | 2 | 1KB |
| 65～128MB | 4 | 2KB |
| 129～255MB | 8 | 4KB |
| 256～511MB | 16 | 8KB |
| 512～1 023MB | 32 | 16KB |
| 1 024～2 047MB | 64 | 32KB |
| 2 048～4 095MB | 128 | 64KB |

2．FAT32 文件系统

FAT32 文件系统提供了比 FAT 文件系统更为先进的文件管理特性，例如，支持超过 32GB 的卷以及通过使用更小的簇来更有效率地使用磁盘空间。作为 FAT 文件系统的增强版本，它可以在容量从 512MB 到 2TB 的驱动器上使用。

FAT 和 FAT32 可以与其他操作系统的文件格式兼容。如果磁盘设置了多重启动配置，很可能需要 FAT 或 FAT32 文件系统。如果用户在同一硬盘上进行 Windows Server 2003 和另一个操作系统配置双重启动，文件系统选择的标准如下：如果安装分区小于 2GB，另一个系统为 Windows NT 较早的版本，将安装分区格式化为 FAT 格式。在大于或等于 2GB 的分区上则使用 FAT32 文件系统。如果在 Windows Server 2003 安装程序中选择使用 FAT 文件系统，并且安装分区大于 2GB，安装程序将自动按 FAT32 格式化。

3．NTFS 文件系统

NTFS 文件系统的设计目标是在很大的硬盘上能够很快地执行诸如读、写和搜索这样的标准文件操作，甚至包括像文件系统恢复这样的高级操作。Windows Server 2003 推荐使用 NTFS 文件系统，它提供了 FAT 和 FAT32 文件系统所没有的全面性、可靠性和兼容性。

NTFS 文件系统包含了公司环境中文件服务器和高端个人计算机所需要的安全特性。NTFS 文件系统还支持对于关键数据完整性十分重要的数据访问控制和私有权限。

Windows Server 2003 使用 NTFS 文件系统，该文件系统在原有的安全特性（如域和用户账户数据库）上又加入了新的特性，如活动目录（Active Directory）、域、文件加密、分布式文件、其他的数据存储模式、磁盘活动的恢复日志、磁盘配额和对于大容量驱动器的良好扩展性。

4．NTFS 和 FAT 的区别

Windows Server 2003 可以采用以上 3 种类型的文件系统，建议在安装 Windows Server 2003 时采用 NTFS 文件系统，否则它的许多功能无法实现。FAT 和 FAT32 很相似，只是 FAT32 更适合于较大容量的硬盘（对于大硬盘来说，最佳的文件系统是 NTFS）。

NTFS 具有 FAT 文件系统的所有基本功能，并且有如下的 FAT 或 FAT32 文件系统所没有的优点：

- 更为安全的文件系统；
- 更好的磁盘压缩性能；
- 支持最大达 2TB 的大硬盘。

### 6.3.3 Windows Server 2003 提供的网络服务

Windows Server 2003 是多任务操作系统，它能够按用户的需求，以集中或分布的方式处理各种服务器应用。它所提供的网络服务包括：

- 文件和打印服务；
- Web 服务器和 Web 应用程序服务；
- 邮件服务；
- 终端服务；

- 远程访问/虚拟专用网络（VPN）服务；
- 目录服务器、域名系统（DNS）、动态主机配置协议（DHCP）服务器和 Windows 系统 Internet 命名服务器（WINS）；
- 流媒体服务。

Windows Server 2003 系统的安装比较简单，在此不做说明，有兴趣的同学可以自行安装学习。在本章的后续课程会讲述其服务的相应安装以及应用。

## 6.4　活动目录服务

活动目录是基于 Windows 的目录服务，目录服务就是将网络系统中的各种网络设备、网络服务、网络账户等资源信息集中起来进行管理，为使用者提供一个统一的清单。Windows Server 2003 通过对目录服务数据库的维护来管理网络上众多的计算机、网络设备、打印设备、共享文件、共享打印、网络账户等基本信息和安全信息，提供对系统资源及服务的跟踪定位，使各种资源和服务对用户透明，用户不必知道资源的具体位置就可以方便地访问它们。

### 6.4.1　活动目录概述

活动目录（Active Directory，AD）的应用起源于 Windows NT 4.0，在 Windows Server 2003 中得到了进一步的发展和应用，它具有信息安全性、基于策略的管理性、可扩展性和可伸缩性。它是一种企业类的目录服务，简化了管理，使用户很容易找到各种资源，提供了非常广泛的特性和功能。

理解活动目录的关键就在于“活动”两个字，正因为这个目录是活动的，所以它是动态的，它是一种包含服务功能的目录，它可以做到“由此及彼”的联想、映射。例如，找到了一个用户名，就可以联想到它的账号、出生信息、E-mail、电话等所有基本信息，虽然组成这些信息的文件可能不在一块儿。同时不同应用程序之间还可以对这些信息进行共享，减少了系统开发资源的浪费，提高了系统资源的利用率。

如果把网络比喻为一本书，活动目录就是书的目录，用户查询活动目录就是查询书的目录，通过目录可以访问相应的网络资源。这时的目录是活动的、动态的，当网络上的资源变化时，其对应的目录项就会动态更新。

### 6.4.2　域及域控制器

活动目录的逻辑结构非常灵活，它为活动目录提供了完全的树状层次结构视图，如图 6-1 所示。逻辑结构为用户和管理员查找、定位对象提供了极大的方便。活动目录中的逻辑单元包括域、组织单元（Organizational Unit，OU）、域树、域林。

#### 1．组织单元

组织单元（OU）是用户、组、计算机和其他对象（也可以包含其他的组织单元）在活动

目录中的逻辑管理单位。OU 可以包含各种对象，如用户账户、用户组、计算机、打印机甚至可以包含其他的 OU，就好像文件夹下面可以包含子文件夹一样。这里的组织单元就是活动目录的一种文件夹。对于一个企业来讲，可以按部门把所有的用户和设备组成一个 OU 层次结构，也可以按地理位置形成层次结构，还可以按功能和权限分为多个 OU 层次结构。由于 OU 层次结构局限于域的内部，所以一个域中的 OU 层次结构与另一个域中的 OU 层次结构完全独立。

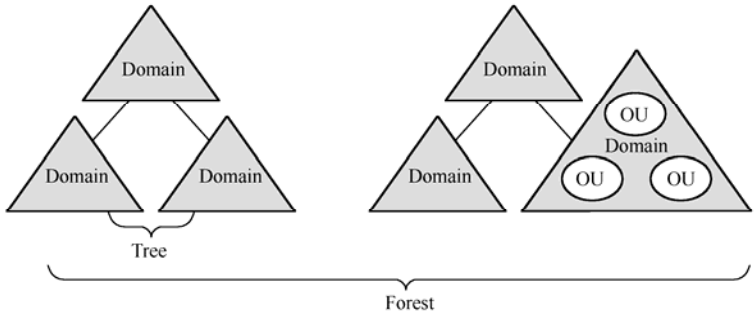



图 6-1　活动目录逻辑单元组

### 2．域

域（Domain）是网络中对计算机和用户等资源的一种逻辑分组。在活动目录中，域是一个或多个组织单元的管理单位，是一个网络安全边界。域管理员只能管理域内资源，除非其他的域赋予他管理权限，它才能够访问或者管理其他的域。每个域都有自己的安全策略，以及它与其他域的安全信任关系，如图 6-2 所示。

### 3．域树

当多个域通过信任关系连接起来之后，所有的域共享公共的表结构（Schema）、配置和全局目录（Global Catalog），从而形成域树。域树由多个域组成，这些域共享同一个表结构和配置，形成一个连续的名字空间。树中的域通过双向信任关系连接起来。活动目录包含一个或多个域树。

域树中的域层次越深级别越低，一个“.”代表一个层次，层次低的域称为子域，层次高的域称为父域，域树中的第一个域称为根域，如图 6-3 所示为域树。

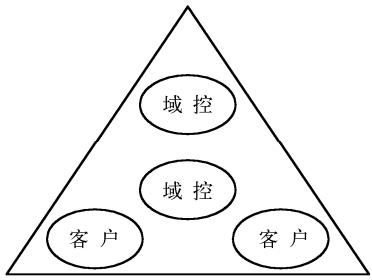



图 6-2　域

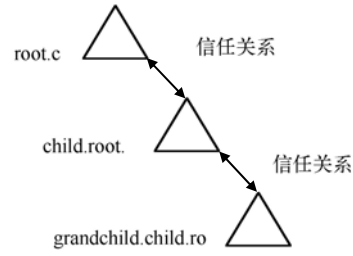



图 6-3　域树

### 4．域森林

域森林是指一个或多个没有形成连续名字空间的域树。域森林中的所有域树共享同一个表结构、配置和全局目录。域林是所有域树通过双向可靠传递信任链接的域树的集合。

### 5．域控制器

安装了活动目录的计算机称为域控制器，对于用户而言，只要加入并接受域控制器的管理，就可以“一次登录，全网使用”（不必在访问每个成员服务器时都要输入不同的账号和密码），可方便地访问活动目录提供的网络资源。对于管理员，通过对活动目录的集中管理就能够管理全网的资源，如图 6-4 所示。

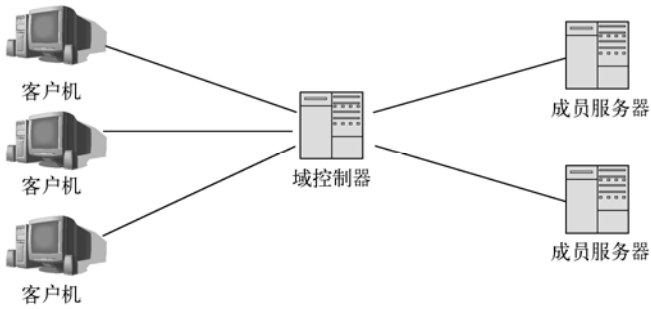



图 6-4　活动目录

一个域中可以有多个域控制器，通过设置，各域控制器之间可以相互复制活动目录。一个域森林中的域控制器之间也可以相互复制活动目录。

### 6．域信任关系

域信任关系是建立在两个域之间的关系，它使一个域中的用户由另一个域中的域控制器验证。验证通过后，便使得一个域中的用户可以访问另一个域中的资源，如图 6-5 所示。

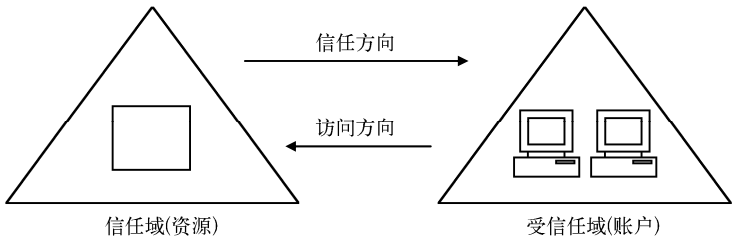



图 6-5　域信任关系

同一个树林中的 Windows Server 2003 域之间会自动建立可传递的信任关系。

非传递的信任关系主要存在于以下域之间：

（1）Windows Server 2003 域和 Windows NT 域之间。

（2）两个森林中的 Windows Server 2003 域之间。

这些域之间的信任关系需要用户手工建立。

## 6.4.3　活动目录的安装

### 1．活动目录的安装

活动目录的安装将使网络中的服务器转换为域控制器。

安装活动目录要启动活动目录安装向导，下面两种方法都可以启动活动目录安装向导。

方法 1：通过执行“开始”→“管理工具”→“管理您的服务器”命令，启动 Active Directory 安装向导。这种方法常用于初次安装活动目录。

方法 2：通过执行“开始”→“运行”→“输入 Dcpromo.exe”命令，启动 Active Directory 安装向导。这种方法常用于活动目录安装完成后，再次启动活动目录安装向导。

下面以方法 1 为例，简要介绍活动目录的安装。

执行“开始”→“管理工具”→“管理您的服务器”命令，打开“管理您的服务器”窗口，然后选择“添加或删除角色”选项，再打开“配置您的服务器向导”中的“预备步骤 ”对话框，单击“下一步 ”按钮，打开“配置选项”对话框，如图 6-6 所示，然后选中“自定义配置”，并单击“下一步”按钮选中“域控制器（Active Directory）”选项，如图 6-7 所示。后续的操作如果不需要更改设置，可以接连单击“下一步”按钮，直至启动 Active Directory 安装向导，如图 6-8 所示。

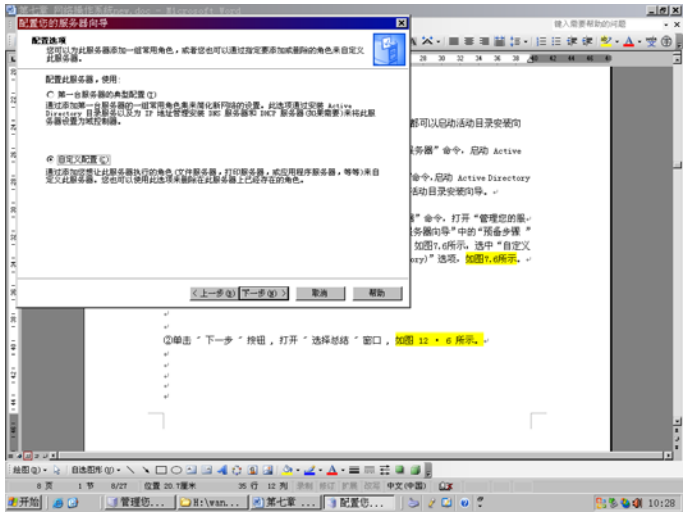


图 6-6　在“配置选项”对话框中选中“自定义配置”

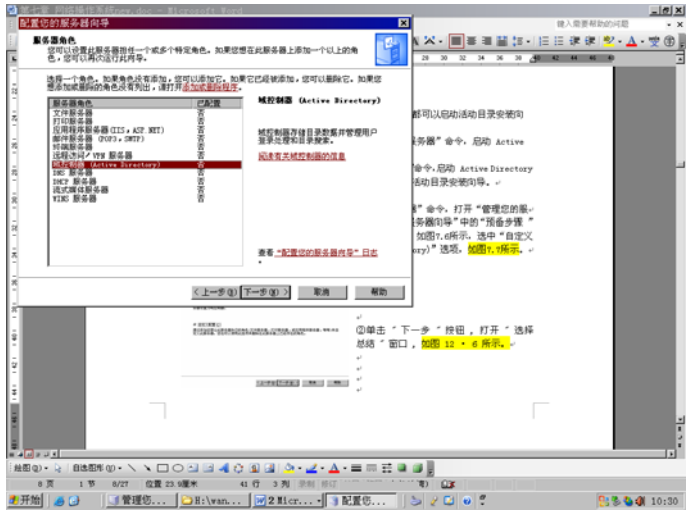


图 6-7　在“服务器角色”对话框中选中“域控制器”选项

之后的步骤按照提示操作，直至单击“完成”按钮。系统提示重新启动计算机。重新启动计算机后，以系统管理员的用户名 administrator 登录。

活动目录安装好以后，Windows Server 2003 的管理工具会发生变化。选择“开始”→“程序”→“管理工具”菜单命令，弹出如图 6-9 所示的“管理工具”快捷菜单。


图 6-8　启动 Active Directory 安装向导


图 6-9　“管理工具”快捷菜单

具体变化如下：

（1）Active Directory 用户和计算机：用于管理活动目录的对象、组策略和权限等；

（2）Active Directory 域和信任关系：用于管理活动目录的域和信任关系；

（3）Active Directory 站点和服务：用于管理活动目录的物理结构（站点）；

（4）域安全策略：类似于工作组下服务器的“本次安全策略”管理工具，但其作用范围是全域，用于制定全域的安全策略；

（5）域控制器安全策略：类似于工作组下服务器的“本地安全策略”管理工具，但其作用范围是域控制器，用于制定域控制器的安全策略。

### 2．服务器的角色转换

运行 Windows Server 2003 的计算机能够按照域控制器、成员服务器和独立服务器三种角色运行，利用 dcpromo.exe 命令可以在各种角色之间更改 Windows Server 2003，以适应所在单位的需要。

域控制器是使用 Active Directory 安装向导配置的运行 Windows Server 2003 的计算机。域控制器存储着目录数据并且管理用户域的交互，其中包括用户登录过程、身份验证和目录搜索。

成员服务器必须是运行 Windows Server 2003 但不是域控制器的注册服务器。

成员服务器不处理用户登录过程，不参与活动目录复制，不存储域安全策略信息。成员服务器一般用做文件服务器、应用服务器、数据库服务器、Web 服务器、证书服务器、防火墙以及远程访问服务器等。由于成员服务器是域的成员，工作时也必须登录到域控制器上，所以它不能脱离域控制器工作。

独立服务器是运行 Windows Server 2003 的计算机，但它不是域的成员。如果 Windows

Server 2003 作为工作组成员安装，则该服务器是独立服务器。独立服务器可与网络上的其他计算机共享资源，但没有活动目录所具有的任何特点。

服务器角色转换的步骤如下：活动目录安装完成后，通过执行“开始”→“运行”命令，打开“运行”窗口，输入 dcpromo.exe，会再次启动活动目录安装向导，可以按照实际要求将域控制器降级为成员服务器，或删除活动目录，将域控制器降级为独立服务器。

**3．活动目录默认结构**

活动目录安装完成后，在“开始”→“程序”→“管理工具”菜单中会生成 3 个以 Active Directory 开头的菜单项，其中，“Active Directory 用户和计算机”命令最常用。打开“Active Directory 用户和计算机”窗口，双击域名展开活动目录，可看到有 5 项活动目录对象，这 5 项活动目录默认结构对象是：

- Builtin：默认的 Windows Server 2003 安全组。
- Computers：默认的计算机账号存储位置。
- Domain Controllers：默认的域控制器的计算机账号存储的位置。
- Foreign Security Principals：外部安全原则，保存外部有信任关系的域的安全标识符（SID）。
- Users：用户账号和组账号的默认位置。

## 6.4.4 用户管理及组管理

**1．组概述**

组可使指派资源权限简单化，用户可以是多个组的成员，一个组可以加入到其他的组中。一个组最多可有5 000个成员。能创建组的用户必须是 Administrators组、Account Operators 组的成员。

（1）组的作用域。组的作用域有“本地组”、“全局组”和“通用组”3 种。

Windows Server 2003 的域有“私有（本机）模式”和“混合模式”两种，“通用组”只在“私有模式”中存在。

- 全局组。全局组主要用于组织相同需求的用户。混合模式下全局组成员可以是同一个域的用户账户，本机模式下全局组成员可以是同一个域的用户账户和其他全局组。

混合模式下全局组可加入到域本地组，本机模式下全局组可加入到任何域的通用组、域本地组、同域全局组中。

全局组可访问本域和所有信任域。

- 本地组。域本地组主要针对资源而设置，包括非域控制器上的资源。混合模式下本地组成员可以是任何域的用户和全局组，本机模式下本地组成员可以是树林中任何域的用户、全局组、通用组、同域的域本地组。

混合模式下本地组不能加入到任何其他组，本机模式下本地组可加入到同一域的其他域本地组。

本地组只能访问自己所在的域。

- 通用组。混合模式下通用组不可使用。本机模式下通用组成员可以是树林中的任何域

的用户、全局组、其他通用组。本机模式下通用组可加入到任何域的本地组和通用组。通用组可访问树林中的所有域。通用组一般不用于单域，它适用于多域环境。

**注意：**

- 在混合域模式下，同类组之间不能嵌套；
- 可将域的混合模式转换为本机模式，但反向转换不行。

（2）组类型。

- 安全组。安全组有安全标识符（SID），用于与安全性有关的功能，如资源权限。也可用于向多用户发送 E-mail 信息，此时功能与分布组相同。
- 分布组。分布组无安全标识符，与安全性无关，不能为其授权，用于群发电子邮件。分布组有时是必要的，因为某些应用程序只能读分布组，如 MS Exchange Server 2000（针对活动目录设计）。
- 安全标识符。安全标识符（SID）由文字和数字组成，它用来唯一标识用户、组、服务、计算机。Windows 2000 控制访问时是使用安全标识符，而并非名字的。

用户或组的安全性标识符不可重用，删除后即使再建同名的用户或组，Windows 2000 也认为是不同的用户或组，因为它们的安全性标识符与原来不同。

（3）组在树林中的使用策略。树林中有许多域，域中组的许可策略可按用户—全局组—本地组分配资源许可。将用户放入某一个全局组中，再将该全局组放入某一个本地组中，最后对该本地组分配资源许可。

如果只有一个单域，则不必设置得这么烦琐，只需将用户放入某一个组中，再对该组分配资源许可即可。

（4）特殊组。Windows Server 2003 内置了一些特殊组，如 Everyone（所有用户，含 guest 用户）、Authenticated Users（所有通过认证的用户，不含 guest 用户）等。

内置的域本地组在活动目录的 builtin 文件夹中，用于在域控制器的活动目录中执行任务，它们位于域控制器上，不可删除。

域定义的全局组在活动目录的 Users 文件夹中，用它们控制域中所有用户更容易，它们只存在于域控制器上。Domain users 组包括所有域用户和 guest 用户。

### 2．创建组

创建组并为组添加成员的步骤如下：

通过执行“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，选中某组织单位，再右键单击该组织单位，选择“新建”→“组”命令，打开“新建对象-组”对话框。在该对话框中输入组名，选择组作用域和组类型，默认情况下，系统将创建全局安全组，如图 6-10 所示。输入组名后，单击“确定”按钮，一个全局安全组便创建好了。

以这样类似的方法还可以创建“本地域”组，这里不再赘述。之后可以右击组名，选择“属性”命令，然后选择“成员”选项卡，如图 6-11 所示，可以添加用户到某一个组中。

### 3．用户账户管理

用户账户是由所有用于定义域用户的信息组成的对象，包括用户名、密码以及该用户账

户所在的组。用户账户可以存储在 Active Directory 中，也可以存储在本地计算机上。


图 6-10　新建全局安全组


图 6-11 “成员”选项卡

（1）用户账户的类型。

① 本地用户账户。本地用户账户建立在 Windows Server 2003 的本地安全数据库内。用户利用本地用户账户只能登录到本机，并且只能使用本机的资源。

② 域用户账户。域用户账户建立在域控制器的 Active Directory 数据库内。用户可以利用域用户账户在任一计算机上登录到域，并访问域中的资源。

当用户利用域用户账户登录时，由域控制器来检查用户所输入的账号名称与密码是否正确。

（2）内置的用户账户。

① Administrator（系统管理员）。Administrator 拥有不受限制的权限，可以管理计算机与域内的设置，如建立、修改、删除用户与组账户，设置用户与组账户的权限，设置安全策略等。

② Guest（客户）。Guest 是临时访问网络或只访问网络一次的用户使用的账户，只有少部分的访问权限。默认情况下，该账户是禁止登录的，如果要使用，必须修改其属性。

（3）用户账户的创建。在创建用户账户时应注意用户登录名和全称必须是唯一的，用户名最多可以包含 20 个字符，可以是大小写字母或者数字；密码最好使用复杂密码。

默认情况下，只有系统管理员才具有管理用户账户的权限，所以建立用户账户之前，必须用 Administrator 账户登录，然后使用“Active Directory 用户和计算机”控制台来建立域用户账户，如图 6-12 所示。

（4）用户账户的管理。用户账户是指由定义 Windows Server 2003 用户的所有信息组成的记录，它包括用户登录所需要的用户名、密码、用户账户具有成员关系的组，以及用户使用计算机和网络时访问资源的权限。

用户账户管理包括设置域用户的属性、域用户账户的复制、删除用户账户、重设用户账户密码、移动用户账户等操作。对于 Windows Server 2003 域控制器，用户账户即域用户账户，受“Active Directory 用户和计算机”管理。有关用户账户的属性对话框如图 6-13 所示。


图 6-12　建立用户窗口


图 6-13　用户属性对话框

## 6.4.5　计算机账户的管理

### 1．计算机账户概述

加入域中且运行 Windows Server 2003 或 Windows NT 的每一台计算机均具有计算机账户。与用户账户类似，计算机账户提供了一种验证和审核计算机访问网络以及域资源的方法。连接到网络上的每一台计算机都应有自己唯一的计算机账户。

### 2．创建计算机账户

（1）在活动目录中创建计算机账户。通过执行“开始”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，选中某组织单位，再右击该组织单位，选择“新建”→“计算机”命令，弹出“新建对象-计算机”对话框，在该对话框中输入客户机的计算机名，如图 6-14 所示。输入计算机名称后按照提示就可以完成计算机账户的创建。

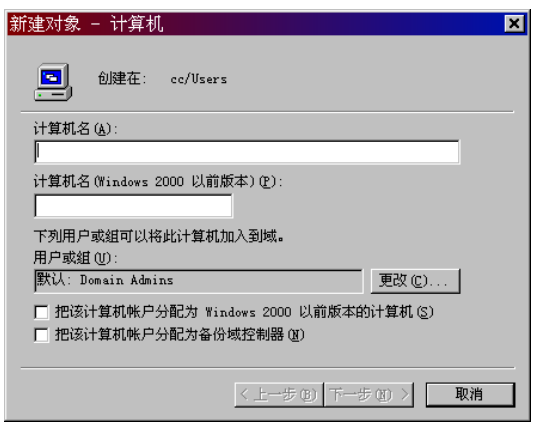



图 6-14　新建计算机账户

（2）将客户机加入到域。要想在活动目录中对客户机进行进一步的控制（如组策略的设

置），还应该在客户机上将客户机加入到域，其操作步骤如下：

① 在 Windows XP 的客户机桌面上右击“我的电脑”图标，选择“属性”命令，打开“系统属性”对话框，如图 6-15 所示，选择“计算机名”选项卡，然后单击“更改”按钮。

② 在打开的“计算机名称更改”对话框中，选择“域”单选钮，并在下面的文本框中输入要加入的域名，如图 6-16 所示。之后按照提示完成加入到某个域的操作。

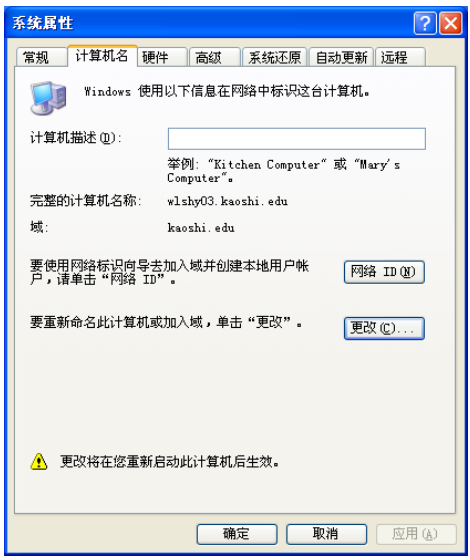



图 6-15　客户机“系统属性”对话框

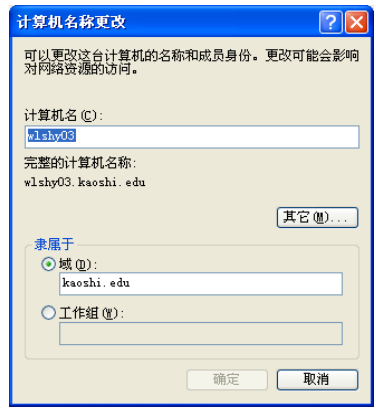



图 6-16　客户机“计算机名称更改”对话框

（3）在活动目录中管理域中的客户机。在服务器的“Active Directory 用户和计算机”窗口中，选中某计算机账户，右击该计算机账户，选择“管理”命令，如图 6-17 所示。在随后打开的“计算机管理”窗口中就可在服务器上对客户机进行相关的管理，需要注意的是，此“计算机管理”窗口中的计算机名是客户机的计算机名。


图 6-17　启动客户机计算机的管理

# 6.5　DHCP 服务

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是 Windows Server 2003 系统内置的服务组件之一。DHCP 服务能为网络内的客户端计算机自动分配 TCP/IP 配置信息（如 IP 地址、子网掩码、默认网关和 DNS 服务器地址等），从而省去网络管理员手动配置相关选项的工作。在使用 DHCP 时，整个网络至少有一台 Windows 服务器上安装了 DHCP 服务，其他要使用 DHCP 功能的工作站也必须设置成利用 DHCP 自动获取 IP 地址。

## 6.5.1　DHCP 概述

一台装有 Windows 操作系统的计算机，可用两种方式设置 IP 地址，一种方式是用户手工设置一个固定的、静态的 IP 地址；另一种方式是从一个 DHCP 服务器上自动地、动态地获得一个 IP 地址。

### 1．手工配置 TCP/IP 的缺点

① 在每一台客户计算机上都要手工输入 IP 地址。
② 不正确的配置可能导致网络问题。
③ 当计算机频繁移动时，有可能要频繁改变 IP 地址的设置，从而加大日常管理开销。

### 2．自动配置 TCP/IP 的优点

① IP 地址被 DHCP 服务器自动分配给每一台客户计算机。
② 保证了客户机总是使用正确的配置信息。
③ 可自动更新客户机配置信息，以反映网络结构的变化。

### 3．DHCP 地址租用过程

在 DHCP 网络中有 3 类对象，分别是 DHCP 客户机、DHCP 服务器和 DHCP 数据库。DHCP 客户机是用来安装并启用 DHCP 客户机软件的计算机。DHCP 服务器是安装 DHCP 服务器软件的计算机。DHCP 数据库是安装在 DHCP 服务器上的数据库，它存储了 DHCP 服务器配置的各种信息，如网络上所有客户机的配置参数、为客户机定义的 IP 地址和保留地址、租约设置信息等。

DHCP 服务器负责为 DHCP 客户端提供 IP 地址，DHCP 客户端采用租用的方式从 DHCP 服务器获得 IP 地址。DHCP 客户端获得地址要经历以下 4 个阶段：

（1）DHCP 客户端发出 IP 租用申请广播。启动 DHCP 客户机时，DHCP 客户端以地址 0.0.0.0（代表本机）为源，255.255.255.255（局域网广播地址）为目标（因此时还没有 IP 地址），发出 IP 租用申请广播。广播信息包含客户机的 MAC 地址和计算机名称。

（2）DHCP 服务器通过 IP 租用提供（包括 IP 地址及租期）广播回应客户端的申请。DHCP 服务器广播的消息中包含以下内容：

- 源地址：DHCP 服务器的 IP 地址。

- 目标地址：因为此时客户机还没有自己的 IP 地址，所以用广播地址 255.255.255.255。
- 客户机地址：DHCP 服务器可提供的一个客户机使用的 IP 地址。

另外还有客户机的 MAC 地址、子网掩码、租约的时间长度和该 DHCP 服务器的标识等。

（3）DHCP 客户端对得到回应的 DHCP 服务器发出 IP 租用选择。

（4）该 DHCP 服务器发回 IP 租用确认（包含被租用的 IP 地址及租期）。

以上过程如图 6-18 所示。

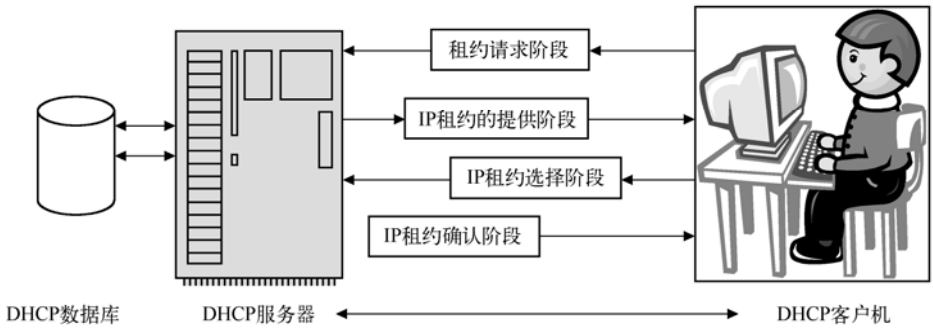



图 6-18　DHCP 网络结构客户机配置过程

#### 4．DHCP 服务器的两种配置方式

① 永久租用。DHCP 客户机从服务器租借 IP 地址后，该地址就永远归该客户机使用。这种方式也称为永久租用，适合于 IP 地址资源丰富的网络。

② 动态地址分配。DHCP 客户机从服务器租借到 IP 地址后，在租约有效期内归该客户机使用，一旦租约到期，IP 地址将被收回，可以供其他客户机使用。该方式适合 IP 地址资源紧缺的网络。

### 6.5.2　DHCP 服务器的安装与配置

#### 1．DHCP 服务器的安装

如果在第一次安装 Windows Server 2003 时没有选择安装 DHCP 服务，可按下列操作添加 DHCP 服务。

① 执行“开始”→“控制面板”命令，弹出“控制面板”窗口，再双击“添加/删除程序”图标，打开“添加或删除程序”窗口，如图 6-19 所示。

② 在“添加或删除程序”窗口左侧单击“添加/删除 Windows 组件”选项，打开“Windows 组件向导”对话框，如图 6-20 所示。

③ 在“Windows 组件向导”对话框中选择“网络服务”选项，单击“详细信息”按钮，打开“网络服务”对话框，选中“动态主机配置协议（DHCP）”复选框，如图 6-21 所示。

④ 单击“确定”按钮，回到“Windows 组件向导”对话框，单击“下一步”按钮，待文件复制完毕，单击“完成”按钮即可。

#### 2．DHCP 服务器的配置

执行“开始”→“管理工具”→“DHCP”命令，打开 DHCP 控制台窗口，双击对应的

计算机名，如图 6-22 所示。得到授权的计算机名左侧图标中是一个绿色的上箭头。


图 6-19　“添加或删除程序”窗口


图 6-20　“Windows 组件向导”对话框

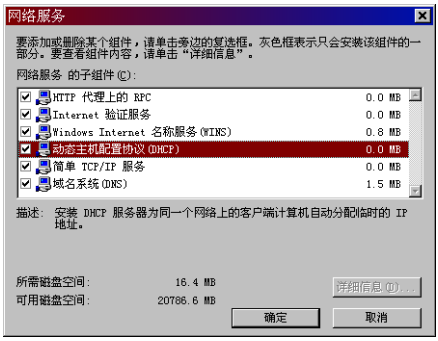



图 6-21　选择安装 DHCP 服务

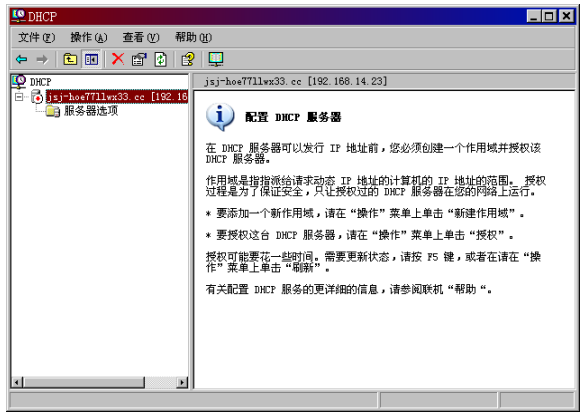



图 6-22　DHCP 控制台

**注意**：在自己设置活动目录后，DHCP 服务器必须先经过超级管理员授权才能使用。如果在计算机名左侧图标中是一个红色的下箭头，则表示该计算机没有得到授权，这时，应单击计算机名，在弹出的快捷菜单中选择“授权”命令。

（1）创建作用域。确认 DHCP 服务器已得到授权后，下一步就应该创建作用域。

① 右击服务器名，在弹出的快捷菜单中选择“新建作用域”命令，打开新建作用域向导，如图 6-23 所示。也可以在“操作”菜单下选择“新建作用域”命令，打开新建作用域向导。

② 在弹出的如图 6-24 所示的“新建作用域向导”对话框中，单击“下一步”按钮。这时将弹出“作用域名”设置选项框，如图 6-25 所示。在“名称”文本框和“描述”文本框中输入描述信息，然后单击“下一步”按钮。

③ 在弹出的如图 6-26 所示的“IP 地址范围”设置选项框中，输入准备分配给客户机的 IP 地址范围的起始地址和结束地址，设置好相应的子网掩码后单击“下一步”按钮。

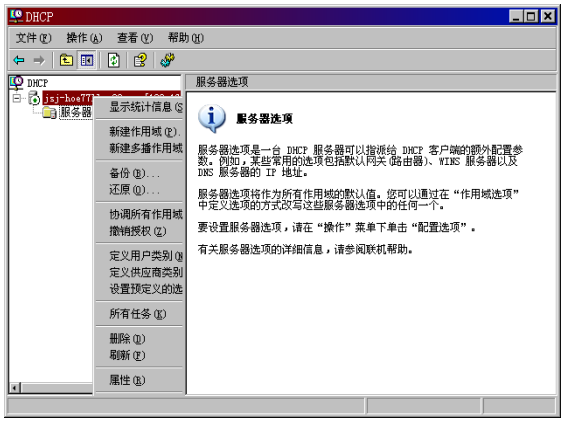



图 6-23　新建作用域

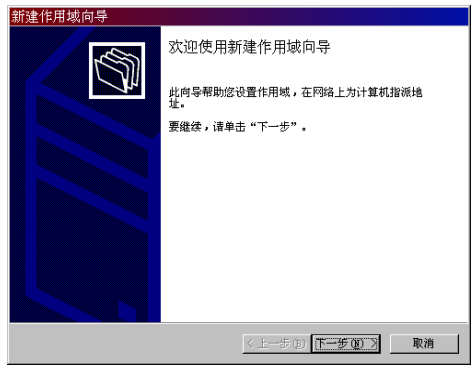



图 6-24　“新建作用域向导”对话框

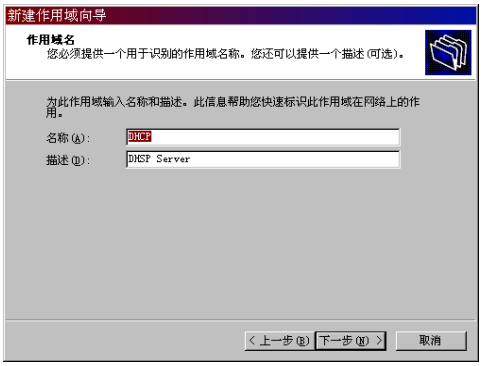



图 6-25　“作用域名”设置选项框

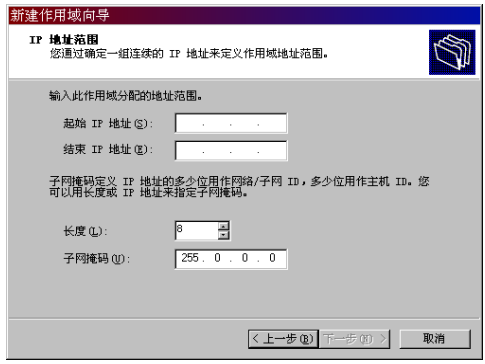



图 6-26　“IP 地址范围”设置选项框

④ 在如图 6-27 所示的“添加排除”设置选项框中，可设置在整个 IP 地址范围中不能分配给客户机使用的部分 IP。在一个网络中要求所有服务器应设置静态 IP，以方便用户访问，故对服务器分配的 IP，应从可分配的 IP 地址池中进行排除，然后单击“下一步”按钮。

⑤ 在弹出如图 6-28 所示的“租约期限”设置选项框中，可设置客户机从 DHCP 服务器租用的 IP 地址可使用的时间长短，默认为 8 天。

在实际工作中，如果网络中的计算机位置经常变动，如笔记本电脑，设置较短的租约期限比较好；如果网络中的计算机位置比较固定，如台式计算机，设置较长的租约期限比较好。

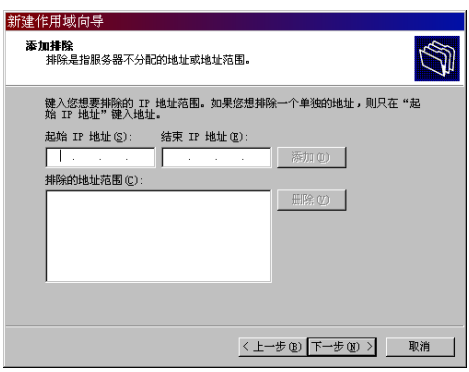



图 6-27　“添加排除”设置选项框

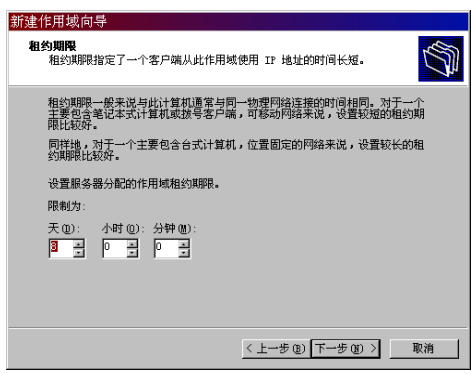



图 6-28　“租约期限”设置选项框

在此后的步骤中，选择默认设置，直到出现“完成”按钮，单击“完成”按钮，结束新建作用域的工作，回到 DHCP 控制台，如图 6-29 所示。

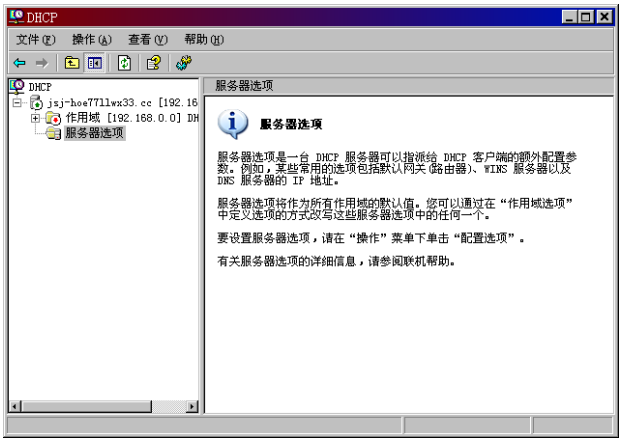



图 6-29　结束新建作用域的 DHCP 控制台

**注意**：此时的作用域左侧图标上有一个红色的下箭头，这表示该作用域没有被激活，必须激活该作用域后，作用域才会生效。

（2）为某些客户机永久分配同一个 IP 地址。DHCP 客户机获得 IP 地址后，当租约期限过期时，DHCP 客户机的 IP 地址将可能发生变化。如果某些客户机因工作需要，要求永久分配同一个 IP 地址，可通过设置“保留”选项来实现。

在 DHCP 控制台中右键单击“保留”选项，从弹出的快捷菜单中选择“新建保留”命令，如图 6-30 所示。

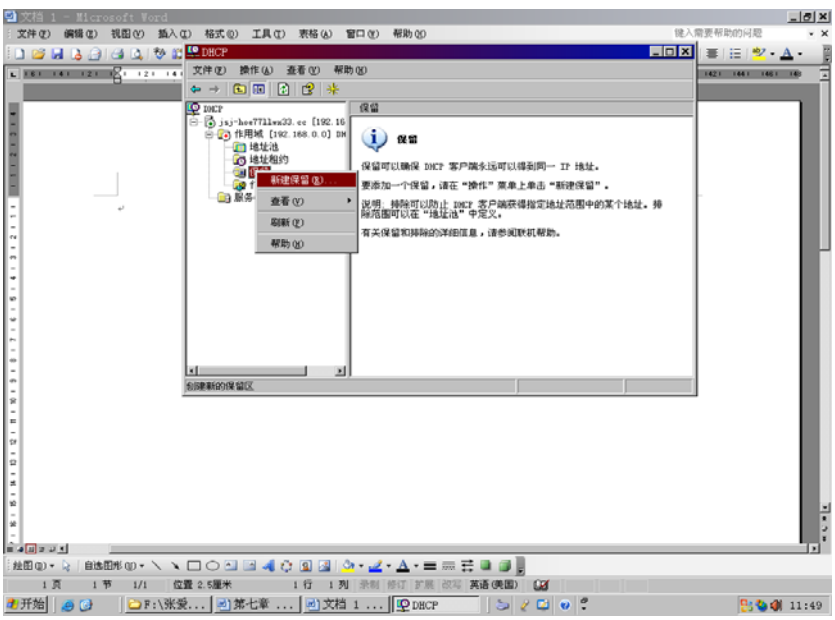



图 6-30　“保留”选项

随后将打开“新建保留”对话框，在“IP 地址”文本框中设置好要永久分配给某主机的

一个 IP 地址，在“MAC 地址”文本框中输入该主机的网卡地址。输入 MAC 地址时，不要输入分隔符（如 OOOC2986EBC5）。客户机的 MAC 地址（网卡物理地址）可在该客户机上的命令提示符下输入命令 ipconfig/all 得知。

设置完成后，单击“添加”按钮，再单击“关闭”按钮。

（3）配置 DHCP 选项。DHCP 服务器不仅可为客户机自动分配 IP 地址，还可以为客户机自动分配路由器（默认网关）地址及联网经常要用到的一些选项，从而使得客户机上几乎什么 TCP/IP 设置都不用手工完成，就可以正常使用网络。

Windows 支持的 DHCP 自动分配的选项有：路由器、DNS 服务器、DNS 域名、WINS/NBNS 服务器、WINS/NBT 节点类型。

在 DHCP 控制台中，右键单击“作用域选项”，在弹出的快捷菜单中选择“配置选项”命令，如图 6-31 所示。

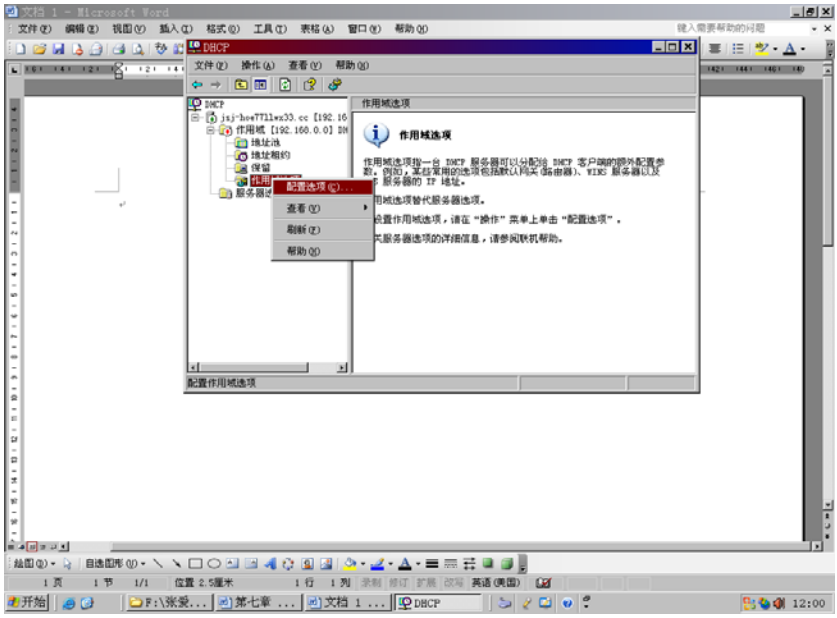



图 6-31　设置“配置选项”

在“作用域选项”对话框中，选中相关选项左侧的复选框，如“路由器”和“DNS 服务器”是经常使用的选项，然后在下面的“IP 地址”文本框中输入相应选项的 IP 地址，单击“添加”按钮，全部设置完成后，单击“确定”按钮。

## 6.5.3　DHCP 客户端的配置与测试

### 1．DHCP 客户机的配置

DHCP 服务器设置好后，客户机使用 DHCP 服务器自动提供的 IP 设置，要进行如下设置：

① 在客户机桌面上，双击“网上邻居”，再右击“本地连接”，选择“属性”命令，如图 6-32 所示。

② 在弹出的如图 6-33 所示的“本地连接 属性”对话框中，有一个“连接后在通知区域

显示图标”的复选框，选中它后，任务栏右侧将会显示一个网络是否连通的图标，通过该图标就可轻易判断出网线是否连好。

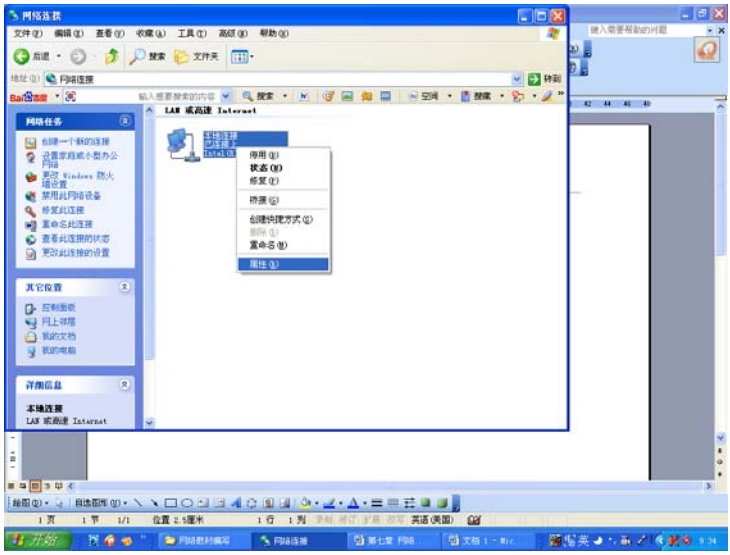


图 6-32　调用网络属性

图 6-33　“本地连接 属性”对话框

③ 在“本地连接 属性”对话框中选择“Internet 协议（TCP/IP）”，再单击“属性”按钮。

④ 在打开的“Internet 协议（TCP/IP）属性”对话框中，选择“自动获得 IP 地址”选项和“自动获得 DNS 服务器地址”选项，如图 6-34 所示。这样，客户机便成为 DHCP 的客户机，可以使用 DHCP 服务器自动提供的 IP 设置。

### 2．DHCP 客户机的测试

DHCP 客户机检查获得的 IP 地址及其他选项的方法如下：

在命令提示符方式下，利用 Ipconfig 命令可检查 IP 地址的获得；利用 ipconfig/all 命令可查看详细的 IP 设置（包括网卡的物理地址），如图 6-35 所示，用 ipconfig/release 命令可释放已获得的 IP 地址；用 ipcofig/renew 命令可重新获得 IP 地址。

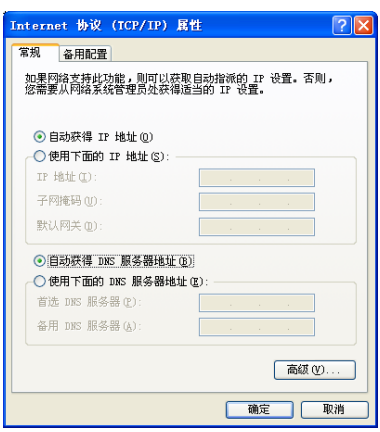


图 6-34　“Internet 协议（TCP/IP）属性”对话框

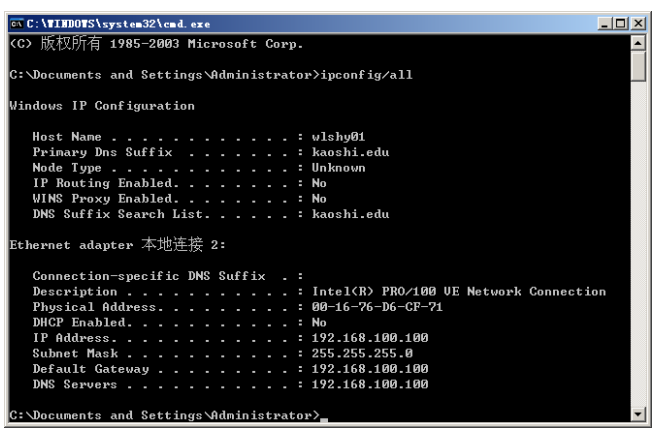


图 6-35　查看详细的 IP 设置

# 6.6 DNS 服务

## 6.6.1 域名系统概述

Internet 上的任何一台计算机都必须有一个 IP 地址，如果用户知道这些计算机的 IP 地址，就可以使用这些计算机提供的服务。但是，这种通过 IP 地址访问计算机的方法（如 http://210.92.33.24），既枯燥又很难将这些计算机与其提供的什么样的服务联系起来。另一种方法，如访问新浪网站用 http://www.sina.com.cn，就是用一些容易记忆的域名来代替枯燥数字代表的网络服务器的 IP 地址。

在网络上，专门有一些计算机来完成“IP 地址”和“域名”之间的转换工作，这种工作就称为域名解析，而完成这项工作的计算机就称为 DNS（Domain Name Server）服务器。

### 1．DNS 命名格式

例如，http://www.sina.com.cn 就是 DNS 的命名格式，其中 http 为超文本传输协议，用于传送网页；www.sina.com.cn 为完全有效域名（FQDN），FQDN 即计算机的全称域名或计算机的全名；www 为主机名，sina.com.cn 为区域名。

### 2．DNS 域名称空间

DNS 域名称空间是定义用于组织名称的域的层次结构的，由名字分布数据库组成，是负责分配、改写、查询域名的综合性服务系统。

域名系统最高级为根域（名为“.”），负责接受所有的 DNS 查询，由 Internet Network Center（InterNIC）管理，InterNIC 承担划分域名空间和登记域名的职责。

根域的下一级称为顶级域，顶级域有的按组织来划分，如 com 代表商业组织、net 代表网络服务机构、edu 代表教育科研部门、gov 代表政府机构；有的按地理位置来划分，如 cn 代表中国、jp 代表日本。

顶级域下的某个特定的组织，称为二级子域，如 edu.cn 代表中国教育科研网。

子域是二级域下面所创建的域，如 tsinghua.edu.cn 代表清华大学。

### 3．域名的解析过程

DNS 服务可将域名解析成 IP 地址。当用户输入域名后，DNS 将按如下过程进行解析：

① 检查是不是本机名；

② 查询本机的 HOSTS 文件（\winnt＼System32\drivers\etc\hosts）；

③ 查询 DNS 服务器；

④ 查询 WINS 服务器（若 DNS 与 WINS 进行了集成）。

主机名是计算机在域中的名称，计算机名是每台计算机的实际名字，这两种名字在 Windows 2000 中已得到统一。

### 4．域名的搜索方式

域名的搜索方式包括正向搜索和反向搜索。

① 正向搜索：名字到 IP 地址的解析。一般只配置正向搜索区域。

② 反向搜索：IP 地址到名字的解析。

### 5．DNS 区域

区域（Zone）是域名空间中一个连续的部分，一个 DNS 服务器上可驻留多个区域，用于分布负荷或容错。

① 主要区域：可读/写，存于文本文件中。

② 辅助区域：复制标准主区域的内容，是只读的，主要作用是分布负荷。

③ 存根区域：存根区域只包含标识该区域的权威 DNS 服务器所需的资源记录。

④ 在 Active Directory 中存储的区域：只能在活动目录的域控制器上创建；存于活动目录中，随活动目录复制时自动更新；它可以简化配置，使用更方便。

在活动目录中存储的区域数据作为一个活动目录对象被存储或被复制。

它的优点是：不存在单点失败问题，具有容错功能；单一的复制拓扑结构，与活动目录复制一起进行；可靠的动态更新。

主要区域与在 Active Directory 中存储的区域之间可以进行转换。

## 6.6.2　DNS 服务器的安装与配置

### 1．DNS 服务的安装

如果在第一次安装 Windows Server 2003 时没有选择安装 DNS 服务，则可再按下列操作添加 DNS 服务：

执行“开始”→“控制面板”命令，打开“控制面板”窗口，再双击“添加/删除程序”图标，打开“添加/删除程序”窗口。在该窗口左侧单击“添加删除 Windows 组件”选项，打开“Windows 组件向导”对话框。在该对话框中选择“网络服务”，单击“详细信息”按钮，打开“网络服务”对话框，选中“域名系统（DNS）”复选框，如图 6-36 所示。

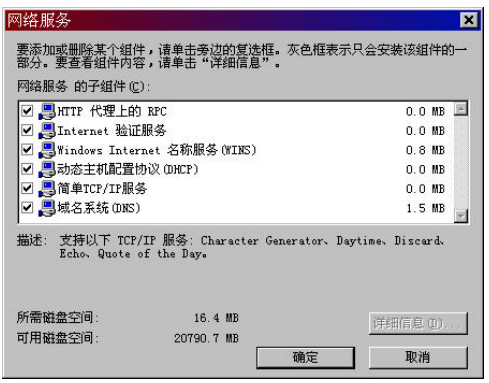



图 6-36　选择安装 DNS 服务

单击“确定”按钮，回到“Windows 组件向导” 对话框，单击“下一步”按钮，待文

件复制完毕，单击“完成”按钮即可。

### 2．DNS 服务器的配置及测试

① 选择“开始”→“管理工具”→“DNS”命令，打开 DNS 控制台，在 DNS 控制台中双击服务器名，如图 6-37 所示。

② 选中“正向查找区域”选项并右击，选择“新建区域”命令，如图 6-38 所示。

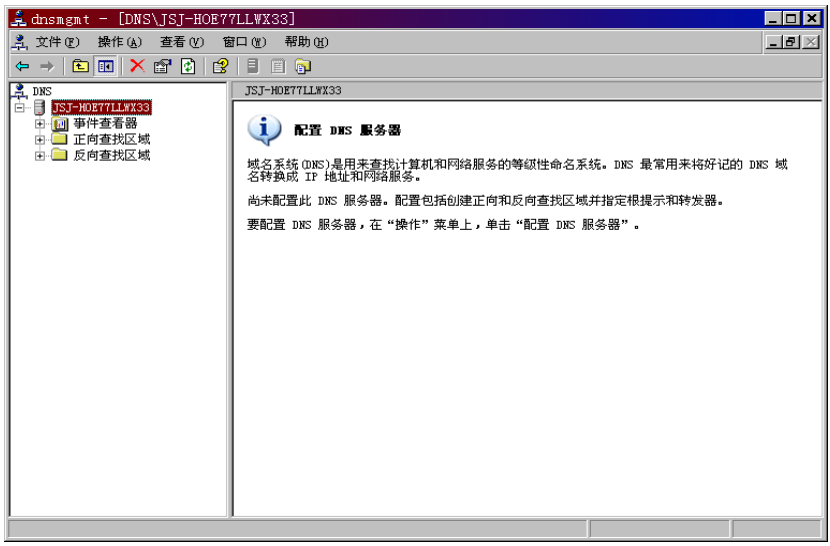



图 6-37　DNS 控制台

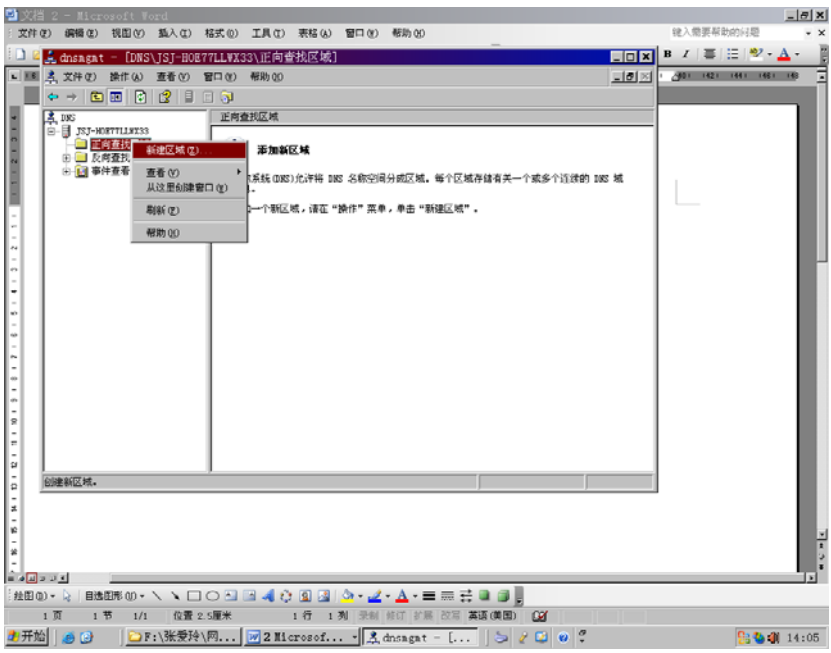



图 6-38　开始新建区域

③ 在随后打开的“新建区域向导”的“欢迎使用新建区域向导”对话框中，单击“下一步”按钮，打开“区域类型”选项框，如图 6-39 所示。

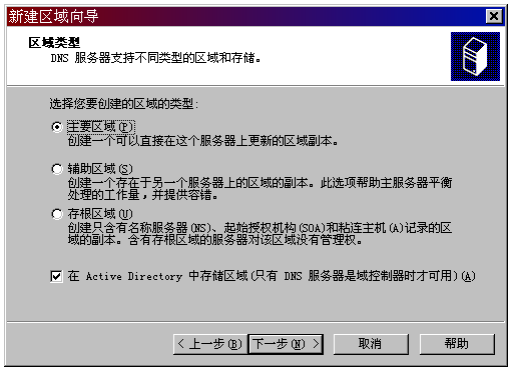



图 6-39 “区域类型”选项框

④ 如果这是网络中第一台 DNS 服务器，则应选择“主要区域”选项或“Active Directory 集成的区域”选项，如果还没有创建活动目录，则“Active Directory 集成的区域”选项不可选。

如果这是网络中第二台 DNS 服务器，则可以选择“主要区域”选项，也可以选择“辅助区域”选项。

在此选择“主要区域”选项，单击“下一步”按钮，进入“区域名”设置对话框，在此后的步骤中可以保持默认设置不变，直到出现“正在完成新建区域向导”对话框，单击“完成”按钮，结束新建一个区域的工作。

如果还要新建其他的区域，重复上面的操作即可。

⑤ 当 DNS 区域建好后，选中区域名，再右击该区域名，选择“新建主机”命令，如图 6-40 所示。

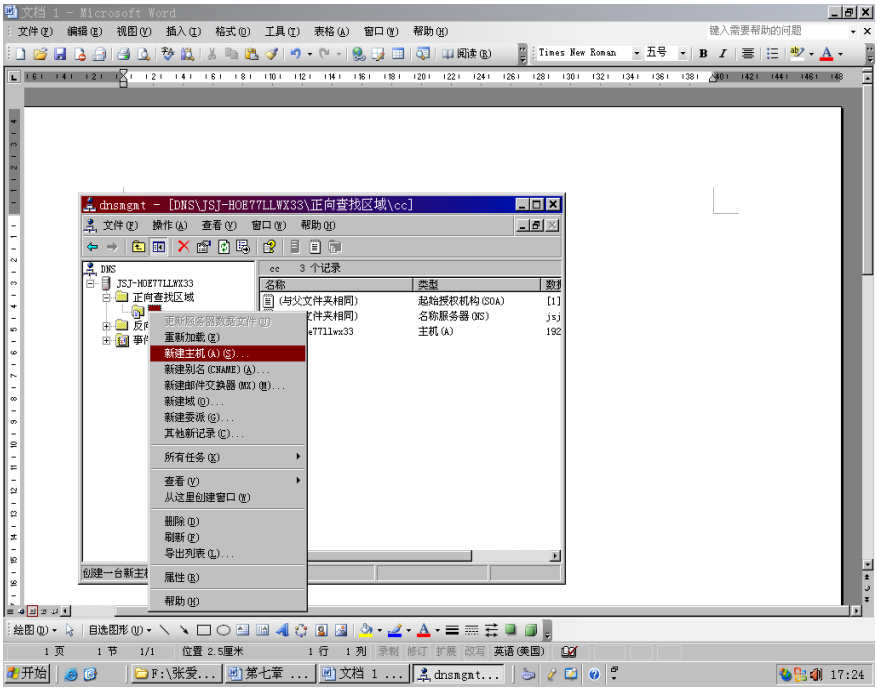



图 6-40　选择“新建主机”

⑥ 在随后打开的“新建主机”对话框中，在“名称”文本框中输入一个主机名，这个主机名可根据需要随意取，不一定是真正的计算机名。在“IP 地址”文本框中输入对应主机的 IP 地址，单击“添加主机”按钮，将出现创建成功的对话框。

DNS 服务器配置完成后，在客户端的 TCP/IP 属性对话框中，要设置 DNS 服务器的地址，或利用 DHCP 服务器动态分配 DNS 服务器的 IP 地址；然后，在命令提示符下输入“ping 完整的域名”命令，以测试 DNS 服务是否生效。

## 6.6.3 DNS 客户端的设置

尽管 DNS 服务器已经创建成功，并且创建了合适的域名，可是在客户机的浏览器中却无法使用 www.mydns.com 这样的域名访问网站。这是因为虽然已经有了 DNS 服务器，但客户机并不知道 DNS 服务器在哪里，因此不能识别用户输入的域名。用户必须设置 DNS 服务器的 IP 地址才行。在客户机“Internet 协议（TCP/IP）属性”对话框的“首选 DNS 服务器”文本框中设置部署好的 DNS 服务器的 IP 地址（本例为 192.168.0.2），如图 6-41 所示。

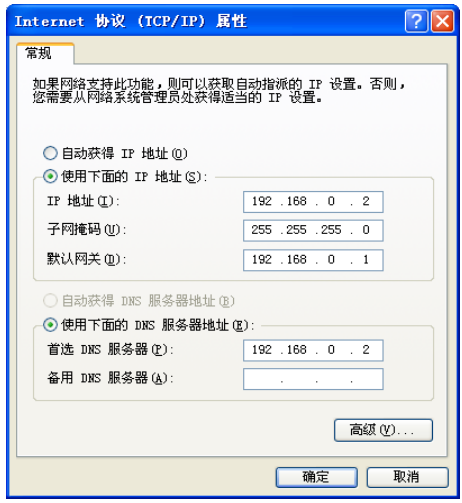



图 6-41 “Internet 协议（TCP/IP）属性”对话框

## 6.6.4 DHCP 与 DNS 的配合

### 1．概述

在 Windows Server 2003 中，DHCP 服务器可对支持更新操作的任何 DHCP 客户机在 DNS 名称空间进行动态更新。当客户机的 IP 地址发生变化时，作用域客户机便可使用 DNS 动态更新协议更新它们的主机名称到地址的映射信息。

### 2．DHCP 与 DNS 的配合

针对 DNS 动态更新配置 DHCP 服务器的方法如下：

① 在 DHCP 控制台中，右击作用域名。选择“属性”命令，如图 6-42 所示。

② 在打开的作用域属性对话框中选择“DNS”选项卡，如图 6-43 所示，在此对各选项进行设置即可。

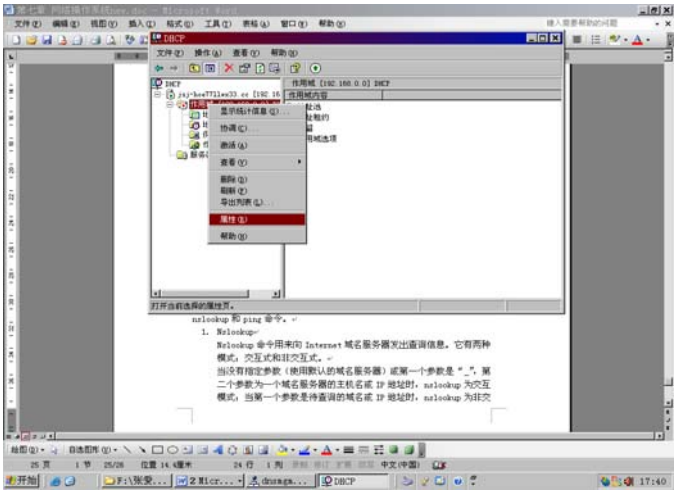


图 6-42　查看/设置 DHCP 作用域属性

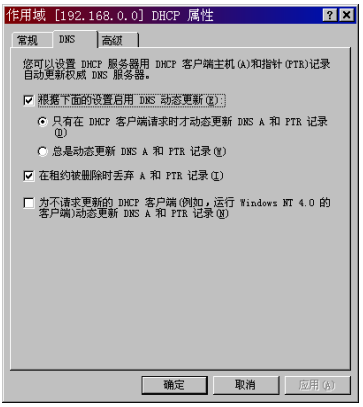



图 6-43　“DNS”选项卡

# 练习 6

## 一、填空题

（1）网络操作系统一般安装在_____上，为网络用户提供使用_____的方法。

（2）网络操作系统除了具备单机操作系统所需的功能外，还应具备：提供高效可靠的网络通信功能；提供多项网络服务功能；提供网络_____管理功能以及对网络_____的管理功能。

（3）目前常用的网络操作系统有_____系统、_____系统、NetWare 操作系统和 Windows 操作系统等。

（4）Windows Server 2003 支持的文件系统包括 FAT16 文件系统、_____文件系统和_____文件系统。

（5）活动目录是基于_____的_____服务。

（6）域是网络中对计算机和用户等资源的一种逻辑分组，是一个网络_____边界；组织单元是用户、组、计算机和其他对象在_____中的逻辑管理单位。

（7）DHCP 服务能为网络内的_____自动分配_____配置信息，从而省去网络管理员手动配置相关选项的工作。

（8）在网络上，专门有一些计算机来完成_____和_____之间的转换工作，这种工作就称为域名解析。

## 二、选择题

（1）Internet 域名中的类型.com 所代表的单位性质是（　　）。

A．商业部门　　B．教育部门　　C．国家机关　　D．网络机构

（2）互联网上的每种服务都基于一种协议，WWW 服务是基于（　　）协议的。

A．FTP　　B．SMTP　　C．HTTP　　D．POP

（3）安装了 Windows Server 2003 的域之间的信任关系是一种（　　）信任关系。

A．单向　　B．双向　　C．多向　　D．任意

（4）DHCP 服务器负责为（　　）提供动态 IP 地址。

A．独立服务器　　B．DHCP 客户端

C．域控制器　　D．成员服务器

（5）DNS 服务可实现的功能是（　　）。

A．将计算机的名字解析为对应的 IP 地址

B．将 IP 地址解析为与之对应的计算机名

C．将 IP 地址解析为 MAC 地址

D．将 MAC 地址解析为 IP 地址

# 第 7 章

# 网络规划设计与综合布线

本章将系统地讲述网络规划设计与综合布线。通过本章的学习，读者能够了解网络规划设计和综合布线的基本概念，网络规划设计的目的、任务及基本步骤，网络层次化结构设计的基本概念，综合布线系统结构，掌握网络布线的实施、网络布线的连接和测试、网络工程的测试与验收等基本方法。

通过本章的学习，应达到如下的学习目标：

（1）了解网络规划的目的、任务及基本流程；

（2）掌握网络的拓扑结构设计、地址分配与聚合设计及冗余设计；

（3）掌握综合布线的基本概念、系统结构及布线实施过程；

（4）了解网络工程的设计、实施、测试与验收等环节。

## 7.1 网络规划

### 7.1.1 网络规划的目的和任务

#### 1．网络规划的目的

通过科学合理地规划能够取得用最低的成本建立最佳的网络，达到较高的性能，提供最优的服务等完美效果。

#### 2．网络规划的主要任务

网络规划的主要任务是对以下指标给出尽可能准确的定量或定性分析和估计。

（1）业务的需求；（2）网络的规模；（3）网络的结构；（4）网络管理需要；（5）网络增长预测；（6）网络安全要求；（7）与外部网络的互联。

### 7.1.2 网络规划的一般步骤

网络规划需要进行的主要工作包括：（1）网络需求分析：包括环境分析、业务需求分析、管理需求分析、安全需求分析。（2）网络规模与结构分析：包括确定网络规模、拓扑结构分析、与外部网络互联方案。（3）网络扩展性分析。

### 1．网络需求分析

网络需求分析包括环境分析、业务需求分析、管理需求分析、安全需求分析。

（1）环境分析。环境分析是指对企业的信息环境基本情况的了解和掌握，如办公自动化情况，计算机和网络设备的数量配置和分布、技术人员掌握专业知识和工程经验的状况，以及地理环境（如建筑物）等。通过环境分析可以对建网环境有个初步的认识，便于后续工作的开展。

（2）业务需求分析。业务需求是企业建网中首要的环节，是进行网络规划与设计的基本依据。那种就网络建网络，缺乏企业业务需求分析的网络规划是盲目的，会为网络建设埋下各种隐患。

业务需求分析的目标是明确企业的业务类型，应用系统软件种类，以及它们对网络性能指标（如带宽，服务质量 QoS）的要求。

通过业务需求分析要为以下方面提供决策依据：

- 需要实现或改进的企业网络功能有哪些？
- 需要技术实现的企业应用有哪些？
- 需要电子邮件服务吗？
- 需要 Web 服务器吗？
- 需要什么样的数据共享模式？
- 需要多大的带宽范围？
- 是否需要网络升级等？

（3）管理需求分析。网络的管理是企业建网不可或缺的方面，网络是否按照设计目标提供稳定的服务，主要依靠有效的网络管理。

网络管理主要包括两个方面：

第一是人为制订的管理规定和策略，用于规范人员操作网络的行为。

第二是指网络管理员利用网络设备和网管软件提供的功能对网络进行的操作。

通常所说的网管主要是指第二点，它在网络规模较小、结构简单时，可以很好地完成网管职能。第一点随着现代企业网络规模的日益扩大，逐渐显示出它的重要性，尤其是网管策略的制订对网管的有效实施和保证网络高效运行是至关重要的。

网络管理的需求分析需要回答以下问题：

- 是否需要对网络进行远程管理？
- 谁来负责网络管理？
- 需要哪些管理功能？
- 选择哪个供应商的网管软件，是否有详细的评估？
- 选择哪个供应商的网络设备，其可管理性如何？
- 怎样跟踪和分析处理网管信息？
- 如何更新网管策略？

（4）安全性需求分析。随着企业网络规模的扩大和开放程度的增加，网络安全的问题日益突出。网络在为企业作出贡献的同时，也为工业间谍和各种黑客提供了更加方便的入侵手段和途径。早期一些没有考虑安全性的网络不但造成了巨额的经济损失，而且使企业形象遭到无法弥补的损坏。一个著名的例子是 Yahoo 网站遭黑：在 Yahoo 举办最新网络安全技术发布会的前夜，黑客入侵 Yahoo.com，更改了主页，一时举世哗然。

企业网络安全性分析要明确以下安全性需求：

- 企业的敏感性数据及其分布情况；
- 网络用户的安全级别；
- 可能存在的安全漏洞；
- 网络设备的安全功能要求；
- 网络系统软件的安全评估；
- 应用系统的安全要求；
- 防火墙技术方案；
- 安全软件系统的评估；
- 网络遵循的安全规范和达到的安全级别等。

### 2．网络规模与结构分析

网络规模与结构分析包括确定网络规模、拓扑结构分析、与外部网络互联方案等。

（1）确定网络规模。确定网络规模即明确网络建设的范围，这是通盘考虑问题的前提。网络规模一般分为以下 4 种：① 工作组或小型办公室局域网；② 部门局域网；③ 骨干网络；④ 企业级网络。

明确网络规模一个明显的好处是便于制订适合的方案，选购合适的设备，提高网络的性能价格比。

确定网络的规模需涉及以下几个方面的内容：

- 哪些部门需要进入网络？
- 哪些资源需要上网？
- 有多少网络用户？
- 采用什么档次的设备？
- 网络及终端设备的数量？

（2）网络拓扑结构分析。网络拓扑结构受企业的地理环境制约，尤其是局域网段的拓扑结构，它与建筑物的结构密切相关。所以，网络拓扑结构的规划要充分考虑企业的地理环境，以利于后期工作的实施，如结构化综合布线工程的设计与实施。

拓扑结构分析要明确以下指标：

- 网络的接入点（访问网络的入口）的数量。
- 网络接入点的分布位置。
- 网络连接的转接点分布位置。
- 网络设备间的位置。
- 网络中各种连接的距离参数。
- 其他结构化综合布线系统中的基本指标。

（3）与外部网络的互联。建网的目的就是要拉近人们交流信息的距离，网络的范围当然越大越好（尽管有时不是这样）。电子商务、家庭办公、远程教育等 Internet 应用的迅猛发展，使得网络互联成为企业建网一个必不可少的方面。

与外部网络的互联涉及以下几方面内容：

- 是否与 Internet 联网？

- 用拨号上网还是租用专线？
- 带宽多少？
- 与专用网络连接吗？
- 需要用户授权和计费管理吗？

**3．网络扩展性分析**

网络的扩展性有两层含义，其一是指新的部门能够简单地接入现有网络；其二是指新的应用能够无缝地在现有网络上运行。可见，在规划网络时，不但要分析网络当前的技术指标，而且还要估计网络未来的增长，以满足新的需求，保证网络的稳定性，保护企业的投资。

扩展性分析要明确以下指标：

- 企业需求的新增长点有哪些？
- 网络节点和布线的预留比率是多少？
- 哪些设备便于网络扩展？
- 带宽的增长估计；
- 主机设备的性能；
- 操作系统平台的性能。

## 7.2 网络设计

### 7.2.1 分层网络设计方法

**1．网络设计的层次结构**

一个大规模的网络系统往往被分为几个较小的部分，它们之间既相对独立又互相关联，这种化整为零的做法是分层进行的。通常网络拓扑设计的分层结构包括 3 个层次，即核心层（Core Layer）、汇聚层（Distribution Layer，又称分布层）和接入层（Access Layer），如图 7-1 所示，每一层都有其自身的规划目标及主要任务。

（1）核心层：一个网络的中心工作就是能够进行数据的传送操作，因此，核心层的主要任务就是要确保网络可以高速、可靠地进行数据传输。由于核心层要对许多的用户提供服务，所以应尽可能保证核心层稳定、高效、可靠地工作，能够及时应对可能发生的各种问题。核心层在现实的互联网络中就是通常所说的骨干网，设备多采用核心路由交换机及路由器。

（2）汇聚层：又称分布层，它处在接入层与核心层之间，起到承上启下的作用。该层的主要任务是为来自接入层的数据提供路由功能，通过一定的路由算法选择一个比较好的通信链路将数据传送出去，同时还必须能够处理一些非正常的数据分组，对这些数据分组进行过滤，保证网络的带宽不被浪费，如果需要，汇聚层还应该提供 WAN 接入功能。汇聚层的设备多以高带宽、高性能、多业务为基本特点，多采用高速智能交换机及路由器。

（3）接入层：它处于三层结构的最低层，也是最靠近用户终端的一层，接入层的主要任务是将数据流量馈入网络，执行网络访问控制，并且提供相关边缘服务。对于企业网来说，大多采用局域网接入，接入设备多使用安全网管型交换机及路由器。

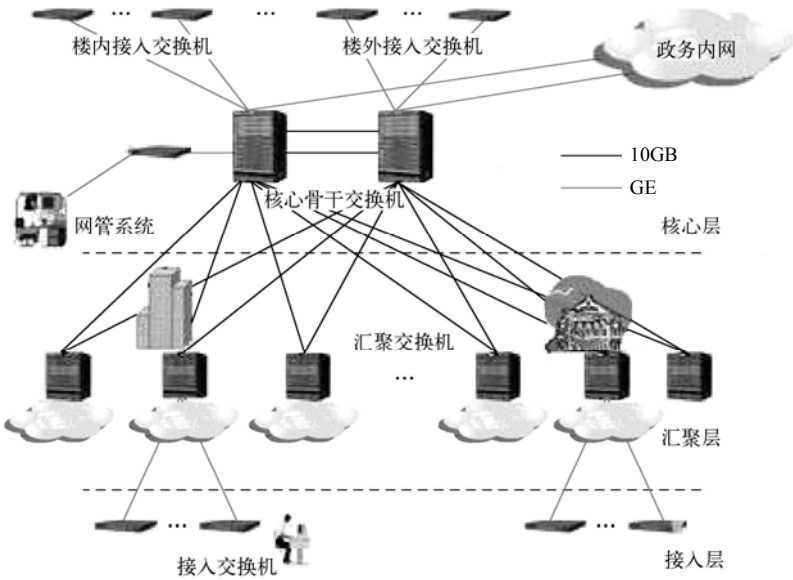



图 7-1　网络设计的三层结构

由上可见，三层结构的划分方法是一个从逻辑高度来看待和理解网络结构的方法和理论，这一思想是由 Cisco 提出的，现已被其他厂商广泛采用，它关注的是整个网络是如何工作的，这对于构建实施网络、进行不同层次的设备选型具有现实的指导意义。

### 2．网络拓扑设计原则

按照分层结构规划网络拓扑时，应遵守以下两条基本原则：

（1）网络中因拓扑结构改变而受影响的区域应被限制到最低程度；

（2）路由器（及其他网络设备）应存储和处理尽量少的信息。

### 3．分层结构的特点

分层拓扑结构的优点：流量从接入层流向核心层时，被收敛在高速的链接上；流量从核心层流向接入层时，被发散到低速链接上。因此接入层可以采用较小的设备，它们交换数据包需要较少的时间，具备了更强的执行网络策略的处理能力。

对于大规模网络规划而言，分层拓扑结构是最有效的，它具有以下特点：

（1）把一个大问题分解成几个小问题，从而容易解决。

（2）将局部拓扑结构改变所产生的影响降至最小。

（3）减少路由器必须存储和处理的数据量。

（4）提供良好的路由聚合或数据流收敛。

分层拓扑结构固有的缺点是在物理层内隐含（或导致）单个故障点，即某个设备或某个失效的链接会导致网络遭到严重的损坏。克服单个故障点的方法是采用冗余手段，但这会导致网络复杂性的增加。

### 4．分层拓扑设计要点

（1）核心层设计要点。

① 不要在核心层执行网络策略：所谓策略就是一些设备支持的标准或系统管理员定制的

规则。例如，一般路由器根据目的 IP 地址发送数据包，但在某些情况下，希望路由器基于源地址、流量类型或其他标准做出主动的决定，这些基于某一标准或由系统管理员配置的规则的主动决定称为基于策略的路由。

牢记核心层的任务是交换数据包，应尽量避免增加核心层路由器配置的复杂程度，因为一旦核心层执行策略出错将导致整个网络瘫痪。

网络策略的执行一般由接入层设备完成，在某些情况下，策略放在接入层与分布层的边界上执行。

② 核心层的所有设备应具有充分的可到达性：可到达性是指核心层设备具有足够的路由信息来智能地交换发往网络中任意目的地的数据包。

在具体的设计中，当网络很小时，通常核心层只包含一个路由器，该路由器与分布层上所有的路由器相连。如果网络更小的话，核心层路由器可以直接与接入层路由器连接，分层结构中的分布层就被压缩掉了。显然，这样设计的网络易于配置和管理，但是其扩展性不好，容错能力差。

（2）汇聚层（分布层）设计要点。汇聚层将大量低速的链接（与接入层设备的链接）通过少量宽带的链接接入核心层，以实现通信量的收敛，提高网络中聚合点的效率，同时减少核心层设备路由路径的数量。总之，汇聚层的主要设计目标包括：

- 隔离拓扑结构的变化；
- 控制路由表的大小；
- 收敛网络流量。

实现分布层设计目标的方法：

- 路径聚合；
- 使核心层与分布层的连接最小化。

（3）接入层设计要点。接入层的设计目标主要包括两个方面，即流量馈入、访问控制。

① 将流量馈入网络：为确保将接入层流量馈入网络，应做到：接入层路由器所接收的链接数不要超出其与分布层之间允许的链接数。如果不是转发到局域网外主机的流量，就不要通过接入层的设备进行转发。不要将接入层设备作为两个分布层路由器之间的连接点，即不要将一个接入层路由器同时连接两个独立的分布层路由器。

② 控制访问：由于接入层是用户接入网络的入口，所以也是黑客入侵的门户。接入层通常用包过滤策略提供基本的安全性保障，保护局部网段免受网络内外的攻击。基本的过滤策略包括地址过滤，例如仅允许来自 10.1.4.0/24 网段的数据通过路由器 A（如图 7-2 所示）；严禁广播源，例如，设置源地址不接收来自 255.255.255.255 地址的广播和 10.1.4.255 网段的广播，广播应被接入层的设备过滤掉。

## 7.2.2 冗余设计

冗余可以简单地理解为备用。

### 1．为什么需要冗余

为什么需要冗余呢？这是因为网络中存在单故障点，即使是强壮的分层结构设计的网络

也存在。所谓网络中的单故障点是指网络中某一台设备或某一条链接发生故障就能导致整个网络瘫痪，发生这种故障的设备节点或链路称为单故障点。

冗余提供备用链接以绕过那些故障点，冗余还提供安全的方法以防止服务丢失。但是如果缺乏恰当的规划和实施，冗余的链接和连接点会削弱网络的层次性和降低网络的稳定性。

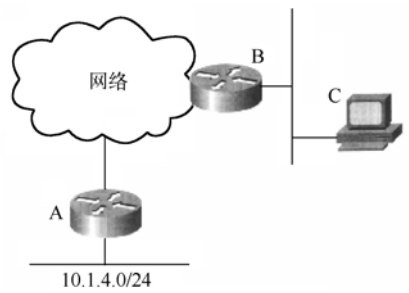



图 7-2　控制访问

### 2．冗余设计要点

下面简要探讨一下如何在分层结构网络中规划冗余。

（1）核心层冗余。核心层冗余规划要综合考虑 3 个目标：减少跳（hop）数，减少可用的路径数量，增加核心层可承受的故障数量。

常见的核心冗余规划有以下两种：

① 完全网状核心层规划：在完全网状规划中，每个核心层路由器都与相关核心层路由器相连接，提供了最大的冗余可能性。它的特点是：有多个到任意目的地的可用路径；正常情况下，到任意目的地要 2 跳；最坏的情况下，最大的跳数为 4。

完全网状核心层规划的优点是提供了最大的冗余度和最少的跳数。缺点是采用完全网状结构的大型网络会产生过多的冗余路径，增加了核心层路由器选择最佳路径的计算量，加大了收敛的时间。

② 部分网状结构的核心层规划：如图 7-3 所示。该方案是折中了跳数、冗余和网络中路径数量的好方案。

正常情况下，该网络中数据传输不会超过 3 跳。当部分网状结构的网络扩大后，相应的跳数依旧比较小。部分网状结构的缺点是：某些路由协议不能很好地处理多点到多点的部分网状规则，因此在某些核心层里最好仍使用点到点的链接。

（2）汇聚层冗余设计。在分布层提供冗余的一种最普通的方法是“双归”，如图 7-4 所示。

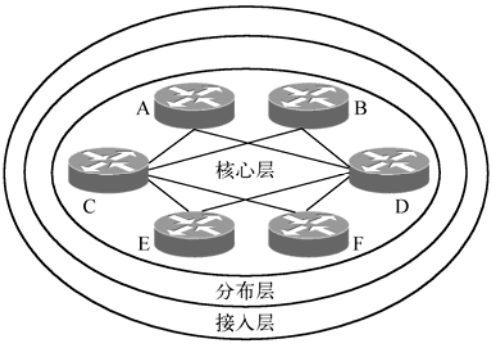



图 7-3　部分网状结构

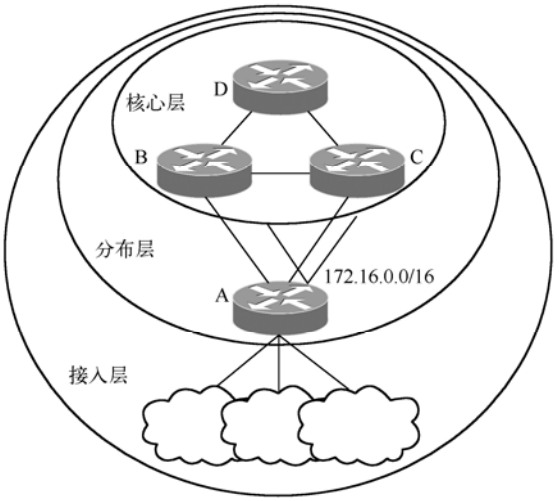



图 7-4　双归接入核心层

双归接入核心层：分布层路由器 A 通过连接到两个核心层路由器接入核心层。双归接入提供了非常好的冗余，当一个路由器或一个链接丢失时，不会削弱路由器后任何目的地的可到达性。

（3）接入层冗余：接入层面临许多与分布层相同的问题。常见的接入层冗余方法也是双归。

### 7.2.3 地址的分配与聚合设计

地址分配是网络规划设计中的要点之一。地址分配方案将直接影响网络的可靠性、稳定性和可扩展性等重要性能。因为地址一旦分配后，其更改的难度和对网络的影响程度将很大。

正确的地址分配方案要充分考虑对以下两个指标的影响：（1）路由表的大小；（2）拓扑结构变化后，相应信息所必须传输的距离。

消除对上述指标影响的有效方法是聚合。下面先来了解聚合设计的方法。

#### 1．聚合设计

在如图 7-5 所示拓扑结构中，无论是 10.1.4.0/24 还是 10.1.7.0/24 链接的失败，都会使路由器 H 重新计算路由表。那么怎样设计才能使核心层路由器 H 不受接入层链接变化的影响呢？聚合是有效的方法，在分布层路由器 G 上将 10.1.4.0/24、10.1.5.0/24、10.1.6.0/24 和 10.1.7.0/24 聚合成一条路径 10.1.4.0/22，并把这一聚合路径只传递给路由器 H。通过聚合，路由器 H 的路由表就可以不再包括路由器 G 左侧的子网细节，路由器 G 左侧的个别链接的改变将不再影响路由器 H 的路由表。另外，聚合减少了路由器 H 必须工作的路径数量，较小的路由表意味着较少的内存、较低的处理请求和更快的收敛过程。

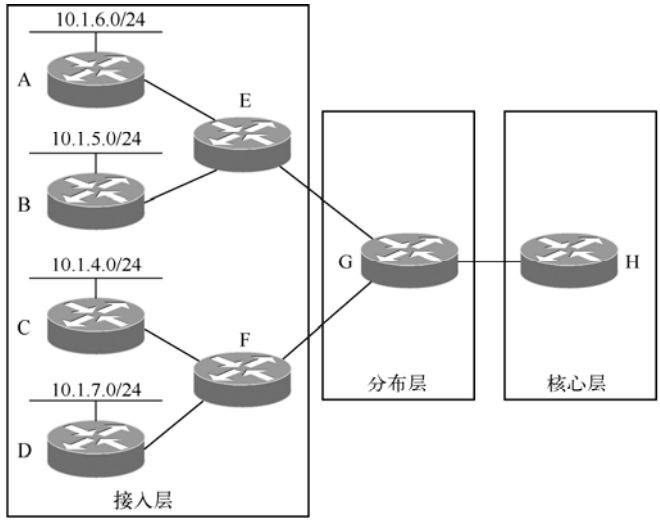



图 7-5　聚合设计

聚合要遵循这样一条规则：只提供网络中必要的拓扑信息，而把不必要的信息隐藏起来。例如，分布层路由器将接入层的每一组目的地聚合为简短的前缀路由，并将之传送给核心层，不再向核心层传送大量的目的地信息。

**注意：**IP 地址后的“/xx”表示所在子网的掩码中从高位算起比特连续为 1 的个数，称为前缀长度，简短的前缀是指前缀中从高位算起的一部分比特，截至何处，要视网段 IP 地址的具体情况而定。

汇聚层是分层网络中最自然的聚合场所。如果拓扑结构发生变化，接入层向核心层传输相应信息之前，接入层里发生的变化会被汇聚层路由器聚合，将受影响的区域缩小在本地分布层范围内。一个典型的例子如图 7-6 所示。同样，从分布层向接入层路由器的聚合可以大大减少这些路由器所必须处理的信息。

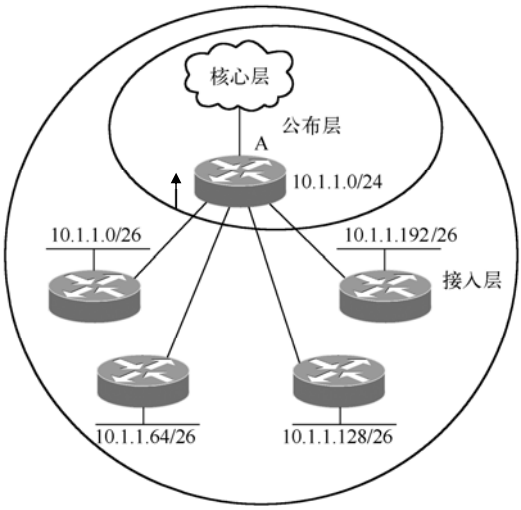



图 7-6　汇聚层聚合

**2．地址分配的一般性原则**

“是否便于聚合”是地址分配的一个基本原则，但该原则的代价是地址的浪费——某些被分配的地址尽管实际没有使用，也不会被重新分配。所以说，网络聚合（稳定性）、扩展性优先考虑的分配原则与节约地址的原则相悖。

为解决上述两难问题，提出地址分配的一般原则，即：（1）使用尽可能大的地址空间，如 IPv6 地址空间；（2）留下空间以供将来扩展。

## 7.3　综合布线技术

### 7.3.1　综合布线概述

**1．综合布线系统的含义**

综合布线系统是一个模块化、灵活性极高的建筑物或建筑群内的信息传输系统，是建筑物内的“信息高速公路”。它既使语音、数据、图像通信设备和交换设备与其他信息管理系统彼此相连，又使这些设备与外部通信网络相连接。它包括建筑物到外部网络或电信局线路上的连线点与工作区的语音或数据终端之间的所有线缆及相关联的布线部件。综合布线系统如

图 7-7 所示。

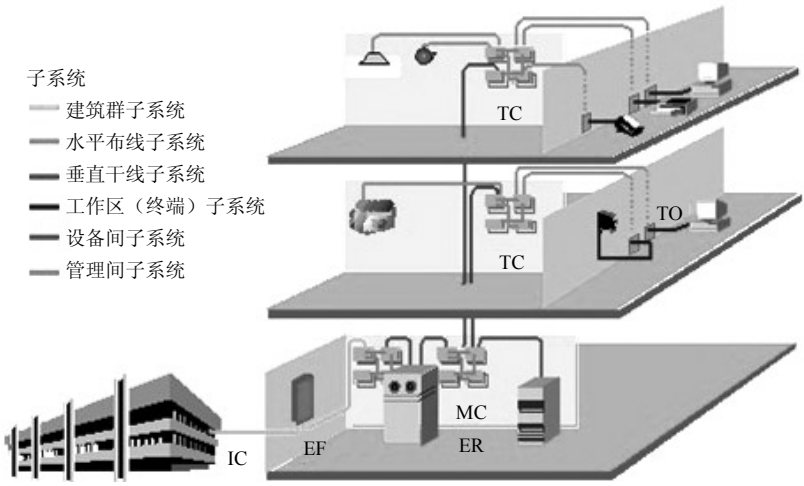



图 7-7　综合布线系统

### 2．综合布线系统标准

综合布线系统的建设通常要遵守相应的标准和规范。随着综合布线系统技术的不断发展，与之相关的综合布线系统的国内和国际标准也更加规范、标准和开放。国际和国内的各标准化组织都在努力制定新的布线标准，以满足技术和市场的需求，标准的完善又会使市场更加规范化。

目前，主要的标准体系有我国的国家标准（GB 50311—2007）、国际标准（ISO/IEC 11801）、美国标准（ANSI/TIA/EIA 568A）、欧洲标准（EN 50173）。制定综合布线标准的主要国际组织有国际标准化组织（ISO/IEC）、北美的工业技术标准化委员会（EIA/TIA）、欧洲标准化委员会（CENELEC）等。

常用的综合布线系统标准有如下几种：

（1）EIA/TIA 568A　《商用建筑通信布线标准》；

（2）EIA/TIA 569　《商业建筑电信通道和空间标准》；

（3）ISO/IEC 11801　《用户建筑综合布线》；

（4）EIA/TIA TSB－67　《非屏蔽双绞线系统传输性能验收规范》；

（5）EN 50173 系列　欧洲标准；

（6）CECS 72—1997　中国工程建设标准化协会《建筑与建筑群综合布线系统工程设计规范》

（7）CECS 89—1997　中国工程建设标准化协会《建筑与建筑群综合布线系统工程施工及验收规范》

（8）GB 50311—2007　国家标准《综合布线系统工程设计规范》

GB 50312—2007　国家标准《综合布线系统工程验收规范》

国家新标准是在 2000 版标准的基础上总结经验，重新编写出来的，它更加完善，更加实用，更具可操作性，更加符合目前行业的发展。新标准注入了相当多的新内容，特别是设计规范方面，对绞电缆部分做了更系统化的修改；在光纤部分，内容更详细；对综合布线系统

的管理、垂直干线电缆的配置、电气防护等内容给出了比较科学的规定。验收标准的内容完善了许多。

新标准的编写遵循了以下主导思想：一是和国际标准接轨，以国际标准的技术要求为主；二是内容符合国家的法规政策，满足电信业务竞争的机制要求；三是规范的内容更贴近工程实际应用。

新的相关标准有：

（1）从 2009 年 6 月 1 日起实施的国家标准《电子信息系统机房设计规范》GB 50174—2008：主要定义了机房分级与性能要求、机房位置及设备布置、环境要求、建筑与结构、空气调节、电气技术、电磁屏蔽、机房布线、机房监控与安全防范、给水排水等方面的要求，并对防火、接地等做了强制要求；

（2）《高层民用建筑设计防火规范》GB 50045－95（2005 年版）；

（3）《建筑设计防火规范》GB J16—87（2001 年版）；

（4）《建筑室内装修设计防火规范》GB 50222—95；

（5）《建筑物防雷设计规范》GB 50057—94；

（6）《建筑物电子信息系统防雷技术规范》GB 50343—2004；

（7）《计算机场地技术要求》GB 2887—2000；

（8）《计算机场站安全要求》GB 9361—88。

## 7.3.2　综合布线系统结构

目前，不同的标准对综合布线系统组成的划分不尽相同，大致可以分为两种：一是按 ISO/IEC 11801 标准把综合布线系统划分为建筑群主干布线子系统、建筑物主干布线子系统和水平布线子系统 3 个布线子系统和一个工作区；另一个是按 EIA/TIA 568－A 标准把综合布线系统划分为 6 个子系统，即工作区（终端）子系统、水平布线子系统、管理间子系统、垂直干线子系统、设备间子系统、建筑群子系统，如图 7-7 所示。下面简单介绍 EIA/TIA 568 标准的划分方法。

### 1．工作区（终端）子系统

工作区（终端）子系统又称服务区子系统，简称工作区。它为需要设置终端设备的独立区域，是由 RJ-45 跳线、信息插座及信息插座所连接的设备（终端或工作站）组成的。其中，信息插座有墙面型、地面型、桌上型等多种，由标准模块组成，能够完成从建筑物自控系统的弱电信号到高速数据网和数字语音信号等各种复杂信息的传送。工作区的 UTP 跳线为软线材料，即双绞线的芯线为多股细铜丝。

设计与安装工作区服务子系统时要注意如下几点：

（1）从 RJ-45 插座到计算机之间的连线用 UTP 双绞线，一般小于 5m。

（2）RJ-45 插座须安装在墙壁上或不易碰到的地方，插座区距离地面 30cm 以上。

（3）配线架上的信息模块与信息插座和插头的线缆的制作要采用同一标准，如 EIA/TIA 568A 或 EIA/TIA 568B，不能接错。

（4）确定 I/O 插座的类型。I/O 插座分为嵌入式和表面安装式两种，可根据实际情况，采

用不同的安装式样来满足不同的需要。通常新建筑物采用嵌入式 I/O 插座，而现有的建筑物采用表面安装式的 I/O 插座。

（5）估算 I/O 插座数量。一般给出两种平面图供用户选择：一种是每 10 平方米一个 I/O 信息插座；另一种是 10 平方米两个 I/O 增强型或综合型插座。

（6）用电配置要求。每组信息插座附近宜配置 220V 电源三孔插座，为设备供电，其间距不小于 10cm。暗装信息插座（RJ-45）与其旁边电源插座应保持 20cm 的距离，且保护地线与零线严格分开。

### 2．水平布线子系统

水平布线子系统也称为水平子系统。水平布线子系统从工作区的信息插座开始到管理子系统的配线柜，如图 7-8 所示，它与垂直干线子系统的区别在于：水平布线子系统总是在一个楼层上，仅与信息插座、管理间连接。在综合布线系统中，水平布线子系统由 4 对 UTP 组成，能支持大多数现代化通信设备。如果需要某些宽带应用，则可以采用光纤。

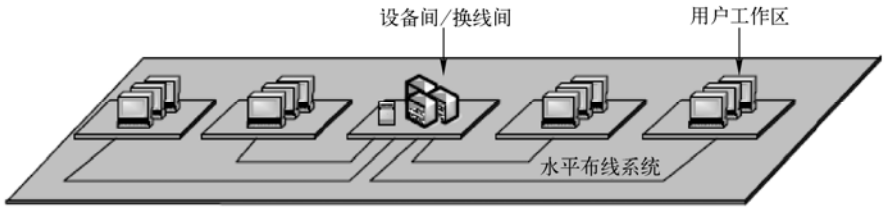



图 7-8　水平布线子系统

水平子系统由用户信息插座、水平电缆、配线设备等组成。综合布线中水平子系统是计算机网络信息传输的重要组成部分，水平主干线通常由屏蔽双绞线（STP）和非屏蔽双绞线（UTP）组成。采用星形拓扑结构，每个信息点均须连接到管理子系统，由 UTP 线缆构成，最大水平距离 90m。水平布线系统的规则如图 7-9 所示。

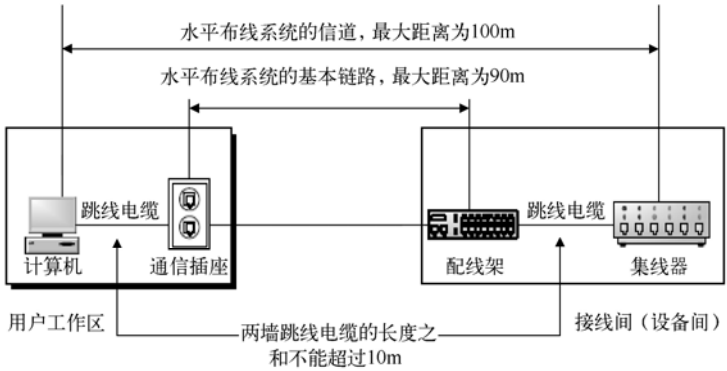



图 7-9　水平布线子系统的规则

目前，综合布线的水平电缆多采用超五类、六类双绞线。工程实践中，计算所需水平电缆长度的一般方法是：$Y$（电缆总长度）=信息点数 × 平均电缆长度= 501× (90+25) ÷ 2 × 1.1= 31 688m，$Y$ ÷ 305m/箱=103 箱。

**说明：**

① 每根水平电缆平均长度按（最长+最短）÷2×1.1 计算。

② 每标准箱为 305m。

③ *Y*÷305M/箱= *Y*/305 箱，订购 *Y*/305 箱非屏蔽双绞线。

水平子系统设计步骤：

① 确定路由；

② 确定信息插座的数量和类型；

③ 确定导线的类型和长度；

④ 确定线缆类型；

⑤ 确定线缆长度；

⑥ 订购线缆。

### 3．垂直干线子系统

垂直干线子系统又称干线子系统。垂直子系统提供建筑物的垂直电缆，负责连接管理子系统到设备间子系统。一般都选用光纤或大对数的非屏蔽双绞线，如图 7-10 所示。

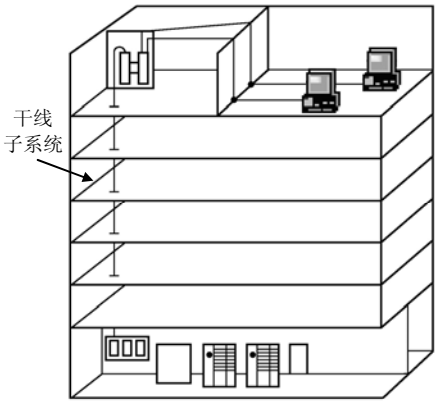



图 7-10　垂直干线子系统

垂直干线子系统由配线设备、干线电缆或光纤、跳线等组成。其任务是将各楼层管理间的信息，传递到设备间并送至最终接口。垂直干线的设计必须满足用户当前的需求，同时又能适合用户今后的要求。为达到此目的，目前多采用超五类 UTP 电缆或光纤，支持数据信息 100/1 000Mbps 的传输，采用五类 25 对非屏蔽电缆，支持语音信息的传输。

垂直主干线安装原则：从大楼主设备间主配线架上至楼层分配线间各个管理分配线架的铜线缆安装路径要避开高 EMI 电磁干扰源区域（如电动机、变压器），并符合 ANSI EIA / TIA 569 安装规定。

大楼垂直主干线缆长度小于 90m 时，建议按设计等级标准来计算主干电缆数量；但每个楼层至少配置两条（CAT5 UTP）做主干。

大楼垂直主干线缆长度大于 90m 时，每个楼层配线间至少配置一条室内八芯多模光纤做主干。主配线架在现场中心附近，保持路由最短原则。

### 4．管理间子系统

管理间子系统也称为配线间，简称为设备间，是整个配线系统的中心单元，是连接垂直干线子系统和水平干线子系统的设备，主要由配线架、集线器、机柜、电源等组成。它的位置确定、安装及环境条件的考虑是否恰当，都直接影响到将来信息系统的正常运行和使用的灵活性。管理子系统（配线室）应尽量靠近弱电竖井旁，而弱电竖井应尽量在大楼的中间，以方便布线并节省投资。

配线间的交连和互连允许将通信线路定位或重定位在建筑物的不同部分，以便能更容易地管理通信线路。I/O 位于用户工作区和其他房间或办公室，使在移动终端设备时能够方便地进行插拔。管理子系统的结构如图 7-11 所示。

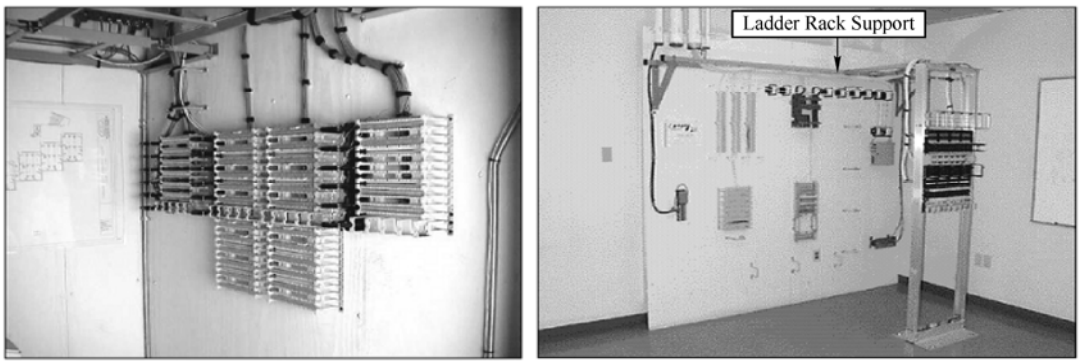



图 7-11　管理间子系统的结构

设计与安装时要注意以下几点：

（1）配线架的配线对数由可管理的信息点数决定。

（2）利用配线架的跳线功能，可使布线系统灵活、功能多样化。

（3）配线柜一般由配线模块、配线架和理线面板组成。

（4）管理子系统应有足够的空间放置配线柜和网络设备。

（5）网络设备须配有安全接地保护系统和功率匹配的净化电源或 UPS 电源。

（6）设备房间内保持一定的温度和湿度，保养好设备。

### 5．设备间子系统

设备间子系统也称设备子系统。EIA/TIA 569 标准规定了设备间的设备布线。它是布线系统最主要的管理区域，所有楼层的数据信息都由电缆或光纤电缆传送至此。通常，此系统安装在计算机系统、网络系统和程控机系统的主机房内。设备间是在每一幢大楼的适当地点设置进线设备，进行网络管理以及管理人员值班的场所。设备间子系统应由综合布线系统的建筑物进线设备、电话、数据、计算机等各种主机设备及其保安配线设备等组成。由建筑群拉来的线缆进入建筑物时应有相应的过流、过压保护设施。

设备间子系统空间要按 ANSI/TIA/EIA 569 要求设计。设备间子系统空间用于安装电信设备、连接硬件、接头套管等。为接地和连接设施，保护装置提供控制环境；是系统运行管理、控制、维护的场所。一个简化的设备间子系统如图 7-12 所示。

**6．建筑群子系统**

建筑群子系统将一个建筑物中的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上。它是整个布线系统中的一部分（包括传输介质）并支持提供楼群之间通信设施所需的硬件，其中有导线电缆、光纤和防止电缆的浪涌电压进入建筑物的电气保护设备。建筑群子系统一般采用架空、埋入地下和地下管道（暖气管道）敷设线缆方式，管道内敷设的铜缆或光纤应遵循电话管道和入孔的各项设计规定。建筑群子系统如图 7-7 所示。

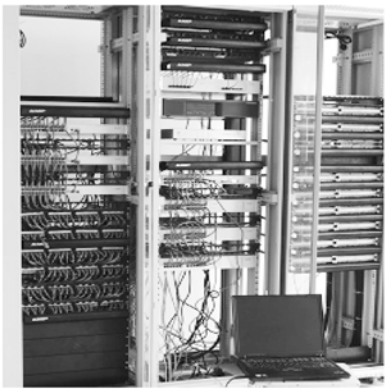


图 7-12　简化的设备间子系统

**7．建筑群骨干光缆设计简例**

某学校的教学楼、科技楼、实验楼、图书馆、办公楼等建筑物之间有大量的语音、数据、图像等传输的需要，由两个及以上建筑物的数据、电话、视频系统光纤组成建筑群子系统。包括大楼设备间子系统配线设备、室外线缆等。光纤的路由主要采用架空光纤、埋入地下和地下管道（暖气管道）敷设光纤。

建筑群子系统介质选择原则：楼和楼之间在 100～5 000m，传输介质为室外多模、单模光纤。可采用埋入地下或架空（4m 以上）方式，需要避开动力线、注意光纤弯曲半径。建筑群子系统施工要点：包括路由起点、终点；线缆长度、入口位置、媒介类型、光纤标志牌。建筑群子系统所在的空间还有对门窗、天花板、电源、照明、接地的要求。

建筑群子系统是连接中心机房和其他建筑楼的配线间的干线。此连接是每个楼宇与中心机房相连的重要主干线路，这里采用多模室外光纤连接。

该校建筑群子系统的几何中心位于科技楼，可将网络中心设在此楼的三层。网络中心即为校园网的主设备间和主配线间，此楼和其他楼宇间的光纤架空距离均小于 550m。因此，采用 50/125 微米的多模光纤、1000Base-SX 模块传输速率可达 1 000Mbps，达到 3 个校区的 1 000Mbps 传输要求，同时为下期工程所有楼宇间 1 000Mbps 传输打好基础。

## 7.3.3　网络设备电力系统设计

电力系统的稳定、可靠也是网络系统正常运行的主要因素之一。设备间要安装配电箱，以保证网络设备运行及维护的供电。室内照明不低于 150lm，主设备室内应提供长延时 UPS 电源，每个电源插座的容量不小于 300W。一般设备间建议安装 1 000VA 的净化电源，以防止过流、过压造成交换机的损坏。

设备室的环境条件为：

- 温度保持在 10～25℃；
- 湿度保持在 30%～50%；
- 通风良好，室内无尘。

# 7.4 网络工程的设计方案、施工、测试与验收

## 7.4.1 网络工程的设计方案

一个完整的设计方案，应包括以下基本内容。

### 1. 设计总说明

设计总说明是对系统工程起动的背景进行简要的说明，主要包括：（1）技术的普及与应用；（2）业主发展的需要（对需求分析书进行概括）。

### 2. 设计总则

设计总则是在这一部分阐述整个系统设计的总体原则。主要包括：（1）系统设计思想；（2）总体目标；（3）所遵循的标准。

### 3. 技术方案设计

技术方案设计是对所采用的技术进行详细说明，给出全面的技术方案。主要包括：（1）整体设计概要；（2）设计思想与设计原则；（3）综合布线系统设计；（4）网络系统设计；（5）网络应用系统平台设计；（6）服务器系统安全策略。

### 4. 预算

预算是对整个系统项目进行预算。主要内容包括列出整个系统的设备、材料用量表及费用；成本分析；以综合单价法给出整个系统的预算表。

### 5. 项目实施管理

项目实施管理是对整个项目的实施进行管理控制的方法。主要包括：（1）项目实施组织构架及管理；（2）奖惩体系；（3）施工方案；（4）技术措施方案；（5）项目进度计划；（6）对业主配合的要求。

### 6. 供货计划、方式

主要描述项目的材料、设备到达现场的计划及供货方式。

### 7. 培训工作计划、方式

指在此项目实施过程中，对业主方相关人员进行的所有培训计划。主要包括：（1）培训的内容；（2）培训的方式；（3）培训的时间安排；（4）培训教师资历等。

### 8. 技术支持及售后服务工作计划、方式

主要内容包括：（1）技术支持方式；（2）技术支持内容；（3）售后现场服务的内容；（4）售后现场服务的时限规定；（5）售后现场服务质量保证措施；（6）公司的其他相关规定。

**9．公司近几年的主要业绩**

列出公司近几年内在综合布线系统工程方面的主要业绩。

**10．公司的资质**

主要包括以下复印件：（1）公司的营业执照；（2）税务登记证；（3）法人代码证；（4）与此项目有关的工程师认证资格证书。

## 7.4.2　网络布线的实施

所谓网络布线的实施，是指将购置的所有网络设备进行安装，使之发挥应有的网络功能。网络布线的实施是在网络设计的基础上进行设备的购买、安装、调试、培训和系统切换工作，是网络工程项目实施方案中综合布线工程施工的主要内容。

**1．网络布线工具**

布线产品主要包括配线架、线缆、信息插座和跳线 4 种，各种产品在布线系统中的应用如图 7-13 所示，其中，线缆用于水平布线、垂直布线和建筑群布线，信息插座用于为用户提供网络接口，配线架用于终结水平布线、垂直布线和建筑群布线，并为网络设备提供接口，跳线用于连接配线架与网络设备，以及信息插座与终端。

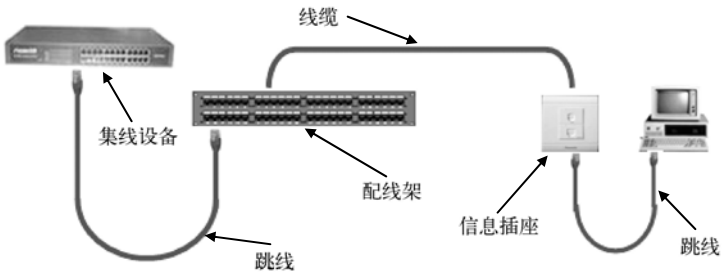



图 7-13　布线产品及其应用

（1）跳线制作工具。在布线时需要制作各种跳线、端接信息插座及配线架，这些工作需要使用专用工具才能制作。如 RJ-45 压线钳、线缆准备工具、偏口钳等。这些工具只用于压制双绞线，不能用于其他用途。

RJ-45 压线钳：如图 7-14 所示，压线钳可完成剪断、剥皮、压制等全部操作。一侧有刀片的地方称为剪线刀口，用于将双绞线剪断，或用于修剪不齐的细线；双侧有刀片的地方，称为线缆准备工具口，用于将双绞线的外层绝缘皮剥下；一侧有牙且对应一侧有槽的地方，称为压线槽，用于将 RJ-45 水晶头上的金属片（针）扎到双绞线中的铜线上。

线缆准备工具：线缆准备工具也称为剥线刀，如图 7-15 所示，它的主要功能是剥掉双绞线外部的绝缘层，在剥皮时不仅比压线钳快，而且还相对安全，一般不会损坏到铜线外的绝缘层。

偏口钳：偏口钳的作用仅是剪取适当长度的网线，以及剪齐并剪去过长的线头，而且仅仅与高级压线钳配套使用。

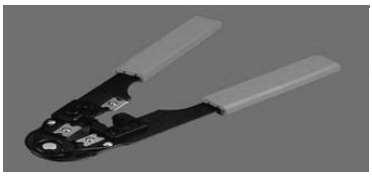



图 7-14　普通 RJ-45 压线钳

图 7-15　剥线刀

（2）信息插座端接工具。在端接信息模块和端接配线架时，除了必须使用线缆准备工具外，还需要用到以下工具：

打线工具：打线工具也称打线刀，用于将双绞线压入信息模块，并剪断多余的线头。

掌上防护装置：掌上防护装置用于在打线时固定模块，并可有效防止模块的意外受损，如图 7-16 所示。

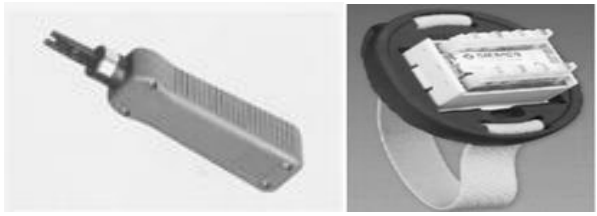


图 7-16　打线工具和掌上防护装置

（3）线缆布放工具。借助于专用的线缆布放工具，可以有效地提高布线速度，保证布线质量，降低线缆布线难度。图 7-17 为双绞线布放支架及线缆钓线。

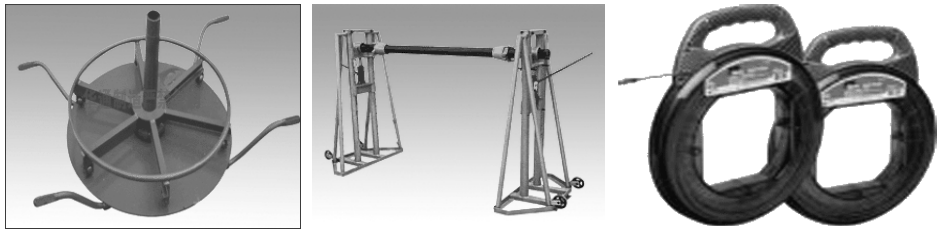


图 7-17　双绞线布放支架及线缆钓线

### 2．双绞线布线实施

双绞线布线作为水平布线的重要组成部分，应用于各种类型的网络布线工程。双绞线布线主要涉及 4 种类型的施工，即水平布线线缆的敷设、工作区信息插座的端接、管理区配线架的端接，以及工作区和管理区跳线的制作。最后，使用跳线依次将计算机连接至信息插座，将配线架连接至集线设备，从而形成完整的数据链路，实现计算机之间的相互通信。

（1）架空布线时应当注意的问题。在吊顶或天花板内进行架空式布线时，应当注意以下问题：

① 加固桥架支撑。当线槽或桥架在水平敷设时，支持加固的间距一般为 1.5～2m。垂直敷设时，应在建筑物的结构上加固，间距一般宜小于 2m。间距大小视线槽和桥架的规格尺寸

和敷设线缆的数量决定，线槽或桥架的规格较大、线缆敷设数量较多，则应缩小支撑加固的间距；相反，则可以放大支撑加固间隔。金属桥架或线槽由于本身重量较大，所以在接头处、转弯处、距端头 0.5m 处及中间每隔 2m 等地方，均应设置支撑构件或悬吊架。

② 避免损伤线缆。为了保护线缆本身不受损伤，在线缆敷设时，应当注意以下几点：布防线缆的牵引力不宜过大，一般应小于线缆允许张力的 80%。在牵引过程中，牵引速度宜慢不宜快，更不能猛拉紧拽。

为防止线缆被拖、蹭、刮、磨等损伤，应均匀设置吊架或支撑线缆的支点，吊挂物或支撑物间距不应大于 1.5m。

在线缆进出天花板处也应增设保护措施和支撑装置。

线缆不应有扭绞、打圈等有可能影响线缆本身质量的现象。双绞线的最小曲率以线缆直径 40mm 为界，小于 40mm 时为线缆外径的 15 倍，大于 40mm 时为线缆外径的 20 倍。

无论是架空布线还是埋入布线，都应当在每条线缆的两端做好标记（简单的方法是用纸条写好编号，然后用透明胶带紧紧缠在线缆上，做防水和防擦处理），以确定该条线缆连接至哪个房间，以便于管理。

（2）埋入式布线时应当注意的问题。当在地板或墙壁内进行埋入式布线时，应当注意以下问题：

① 管槽尺寸不宜太大。预埋暗敷的管路宜采用对缝钢管或具有阻燃性能的 PVC 管，且直径不能太大，否则对土建设计和施工都有影响。根据我国建筑结构的情况，一般要求预埋在墙壁内的暗管内径不宜超过 50mm，预埋在楼板中的暗管内径不宜超过 25mm。金属线槽的截面高度也不宜超过 25mm。

② 设置暗线箱。预埋管线应尽可能采用直线管线，最大限度地避免采用弯曲管道，当直线管线超过 30m 后仍需延长时，应当设置暗线箱，以便于敷设时牵引电缆。如不得不采用弯曲管道时，要求每隔 15m 设置一个暗线箱。金属线槽的直线埋设长度一般不超过 6m，当超过该距离或需要交叉、转弯时，则应当设置拉线盒。

③ 转弯角度不宜过小。当不得不采用弯曲管道时，要求转弯角应当大于 90°，并且要求整个路由的弯管小于两个，更不能出现“S”形弯或“U”形弯。另外，转弯半径也不宜过小，通常情况下，曲率半径不应小于弯管外径的 6 倍。

④ 预放索引绳。暗敷管道内壁应当光滑，绝对不允许有障碍物。为了保护线缆，管口应当加设绝缘套管，管端伸出的长度应为 25～50mm。要求在管路内预放牵引绳或拉绳，以便于线缆的敷设施工。管路的两端还应设有标志，内容包括序号、长度、房间号等，以免发生错误。

⑤ 管槽需留有余量。在管槽中敷设电缆时，应当留有一定的余量，以便于布线施工，并避免线缆受到挤压，使双扭线的扭绞状态不发生变化，保证线缆的电气性能。通常情况下，直线管道的管径利用率（线捆的外径/管道的内径）应为 50%～60%，弯道应为 40%～50%；截面积利用率（暗管内电缆的总截面面积/暗管管径的内截面面积）应为 30%～50%。预埋金属线槽的截面积利用率不应超过 40%。

### 3．制作跳线

所谓跳线，就是两端有 RJ-45 接头的双绞线。跳线在双绞线网络中被大量使用，无论是

计算机与集线设备之间的连接，还是网络设备之间的连接都离不开它。压制跳线是组建双绞线网络必须掌握的一门技术。由于屏蔽双绞线极少在实际中用到，所以，这里简要介绍非屏蔽双绞线跳线的制作。另外，五类、超五类和六类非屏蔽双绞线的制作方式基本相同。

（1）跳线制作材料：跳线制作材料有以下几种。

① 双绞线：制作跳线最重要的材料就是双绞线。由于跳线在整个网络链路中非常重要，对网络传输带宽有重大影响。而跳线的质量主要取决于双绞线的品质，必须选择与布线系统完全相同的产品。

② RJ-45 插头：RJ-45 接头如图 7-18 所示，也称“RJ-45 头”或“水晶头”，它的作用类似于电源线中的插头。所不同的是，每条网线的两端各需要一个 RJ-45 接头。水晶头质量的优劣不仅是网线制作成功的关键之一，也在很大程度上影响着网络的数据传输率。

③ 护套：如图 7-18 所示，护套用于标记线缆。当网络中的跳线较多时，尤其是从配线架跳接到交换机时，由于网络非常多，且都是成束地捆扎在一起，所以在没有标记的情况下，根本无法判断每根跳线所连接的端口。所以，为每条双绞线配上护套，以便于日后的网络管理和故障的判断与排除。

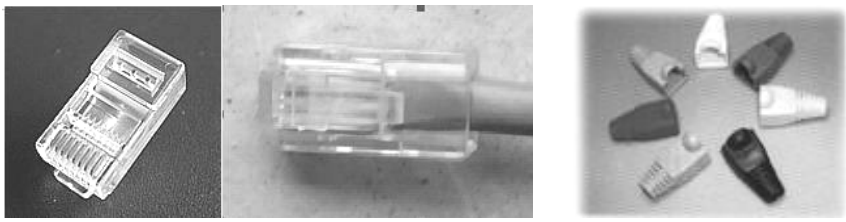


图 7-18　RJ-45 水晶头及护套

（2）T568A 与 T568B 标准。目前，最常使用的布线标准有两种，即 T568A 与 T568B 标准。

T568A 标准描述的线序从左到右依次为：1—白绿、2—绿、3—白橙、4—蓝、5—白蓝、6—橙、7—白棕、8—棕。如图 7-19 所示为 T568A 标准对应的 RJ-45 连接器（水晶头）针脚和线对连接示意图。

T568B 标准描述的线序从左到右依次为：1—白橙、2—橙、3—白绿、4—蓝、5—白蓝、6—绿、7—白棕、8—棕。如图 7-20 所示为 T568B 标准对应的 RJ-45 连接器（水晶头）针脚和线对连接示意图，在网络施工时，可采用任何一种标准，但所有的布线设备及布线施工尽量采用同一标准。

（3）制作跳线。五类和超五类布线系统，可以采用手工制作跳线的方式，以节约布线成本。对于六类布线系统而言，只能够买已经制作好的成品跳线，以保证布线系统的电气性能。

首先，利用压线钳的剪线刀口或偏口钳取适当长度的网线，将线标和护套套入双绞线，以标记该跳线，易于以后的网络管理。再用剥线刀，将双绞线最外层的绝缘层割开，剥下割断的绝缘胶皮，将 4 个线对的 8 根线一一拆开、理顺、捋直，按照规定的线序排列整齐，然后，用压线钳或偏口钳把线头剪平，以使双绞线插入水晶头后，每条线都能良好地接触水晶头中的插针，避免接触不良。

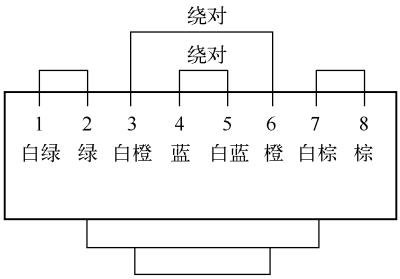



图 7-19　T568A 标准对应的针脚和线对连接示意图

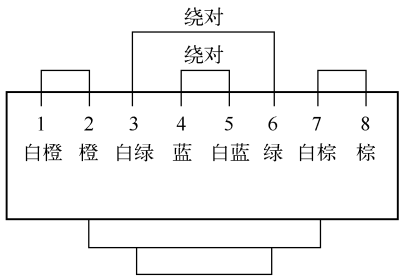



图 7-20　T568B 标准对应的针脚和线对连接示意图

将 8 根线同时沿 RJ-45 内的线槽一直插到顶端，并从水晶头的两个侧面观察是否已经将所有的线对都插至底部，透过水晶头检查一遍线序是否正确。准确无误后，用压线钳将 RJ-45 头的针脚全部压入水晶头内，以使针脚与导线可靠连接。

最后，将护套套在水晶头上，这条网线的一端就算制作好了，然后用同样的方法将双绞线另一端的水晶头压制好，一条网线的制作即告完成。

（4）直通线与交叉线。双绞线两端的线序根据所连接设备的不同而有所不同，经常使用的跳线有两种，即直通线和交叉线。两端 RJ-45 水晶头中的线序排列完全相同时，称为直通线（Straight Cable），即当一端线序从左到右依次为白橙、橙、白绿、蓝、白蓝、绿、白棕、棕时，另一端线序从左到右也是如此。直通线通常适用于计算机到集线设备的连接。

当使用双绞线直接连接两台计算机或连接两台集线设备时，另一端的线序要做相应的调整，即第 1、3 线对调，第 2、6 线对调，制作成的双绞线即为交叉线（Crossover Cable）。例如：一端使用 T568A 标准，而另一端使用 T568B 标准。

### 4．端接信息插座

端接信息模块时，首先把双绞线从布线底盒中拉出，使用偏口钳剪至 20～30cm，使用剥线刀剥除外层绝缘皮，剪除抗拉线。然后，将信息模块置于专用工具或桌面、墙面等较硬的平面上，分开双绞线的 4 个线对，但线对之间不要拆开，按照模块上所指示的色标线序（执行与配线架相同的标准），将导线一一置入相应的线槽内，如图 7-21 所示。通常情况下， 模块上同时标记有 TIA568A 和 TIA568B 两种线序，应当根据布线设计时的规定，与其他连接设备采用相同的线序。

将打线工具的刀口对准信息模块上的线槽和导线，垂直向下用力，听到“喀”的一声，模块外多余的线即被剪断。如果多余的线不能被剪断，可调节打线工具上的旋钮，调整冲击压力，将 8 条导线一一打入相应颜色的线槽中，如图 7-22 所示。

最后，将塑料防尘片沿缺口穿入双绞线，并固定在信息模块上，用双手压紧防尘片，信息模块端接完成。

信息模块端接好后，将信息模块插入信息面板中相应的插槽内，然后用螺钉将面板固定在信息插座的底盒上。

### 5．端接配线架

端接配线架所需工具为剥线刀、偏口钳和打线刀，可以使用普通的打线工具，也可以使用专用的打线工具，相比较而言，前者的工作效率较低。

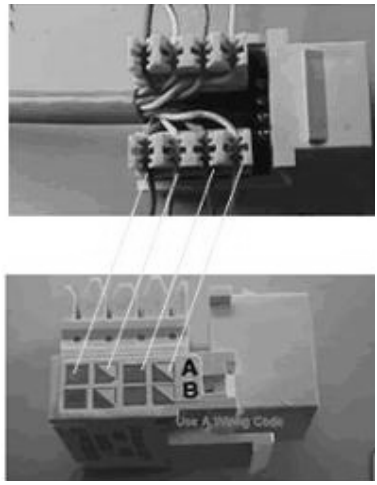



图 7-21　将导线置入模块线槽内

图 7-22　打线

首先，将附送的金属支架安装在配线架上，用于支撑和理顺双绞线电缆；接着，利用尖嘴钳将线缆剪至合适的长度，并用剥线刀剥除双绞线的绝缘层包皮，并剪除抗拉线，依据所执行的标准（执行与信息模块完全相同的标准），依照配线架上的色标，将 4 对线按照正确的颜色顺序一一分开，并全部置入线槽。然后，再利用打线工具端接配线架与双绞线即可。当所有的双绞线端接完成后，将线缆理顺，并利用尼龙扎带将双绞线与理线器固定在一起，并成束地固定在机柜上。

当然，也可以先打好配线架，然后将配线架安装到机柜上。最后，将理线架固定在机柜正面，并利用跳线将配线架与交换机连接在一起，如图 7-23 所示。

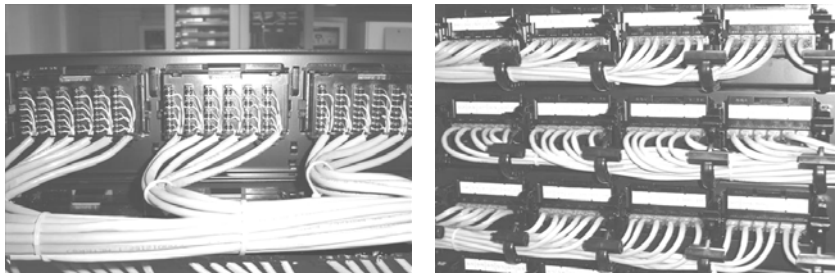


图 7-23　整理后的配线架的背视和正视图

## 7.4.3　网络布线的连接和测试

每一条 Link 链路（即两个压接点之间的链路）安装好，都必须对该链路的性能加以测试，否则等到整个信道安装完成后，再进行检测就相当困难了。

布线施工完成以后，需要使用跳线将计算机连接至信息插座，将配线架连接至集线设备，从而形成完整的数据链路，实现计算机之间的相互通信。

### 1．网络布线的连接

（1）双绞线的连接。网络链路的连接方式及配线架与交换机使用跳线连接的方式，如

图 7-24 所示。

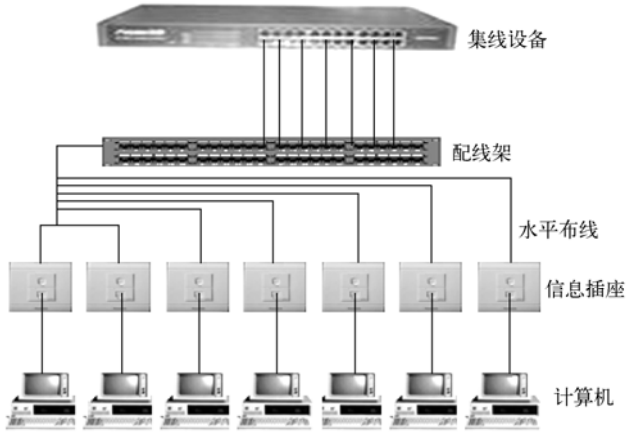



图 7-24　网络链路的连接方式

在连接网络链路时，应注意以下几个方面的问题：

为了便于区别不同楼层、房间或部门的连接，建议采用不同颜色的跳线连接配线架与集线设备，从而便于实现对网络连接的管理。

在配线架端口、跳线两端和信息插座上，都应当使用标签进行标记，并且使每个链路的标记完全一致，从而便于布线系统的日常维护和故障排除。在配线架的标识上，还应当标注楼号和相应的楼层。如果条件允许，可以借助标签打印机实现标签的标准化打印。

在布线实施过程中，一定要做好技术文档的记录，最后绘制布线图纸并存档。技术文档的内容应当包括：布线路由、信息插座的位置与编号、配线架端口与所对应信息点的位置等。

（2）光纤的连接。光纤连接的方式主要有两种，即磨接和熔接。

采用磨接方式，虽然工具设备投入较少，但所需时间较长，且对技术人员和施工环境的要求较高，成功率较低，现已很少采用。

光纤熔接技术是在高压电弧的作用下将两根需要拼接的光纤的端头熔化后连接在一起。采用熔接方式，虽然工具投入较多，但制作速度快，技术人员经过培训即可上岗，且成功率非常高，目前已成为光纤的首选接续方式，熔接时使用的光纤熔接机如图 7-25 所示。

图 7-25　光纤熔接机

在通常情况下，熔接的损耗较小，一般在 0.1dB 以下，并且可以立即从测试屏幕上得到损耗值。但是，在光纤熔接过程中，影响熔接质量的外界因素也比较多，如环境条件（包括温度、风力、灰尘等）、操作的熟练程度（包括光纤端面的制备、电极棒的老化程度）、光纤与尾纤（指一端有光纤连接器的光纤，与光纤连接在一起，从而实现与信息插座和光纤终端盒的连接）的匹配性（包括光纤类型匹配、光纤生产厂商匹配）等。

### 2．双绞线性能测试

对于小型网络或对数据传输速率要求不高的网络而言，只要简单地做一下网络布线的连通性测试即可，使用的工具只需普通的线缆通断测试仪。作为集多种测试功能于一身的网络

测试仪，Fluke MicroScanner Pro （如图 7-26 所示）是专为防止和解决线缆安装问题而设计的，使用线序适配器可以迅速检验 4 对线的连通性，以确认被测线缆的线序正确与否，并识别开路、短路、跨接、串扰或任何错误连接，迅速定位故障，从而确保基本的连通性和端接的正确性。

① 双绞线连通性测试：Fluke MicroScanner Pro 的连通性测试可以测试双绞线跳线的连通性、水平布线中配线架至信息插座的连通性和整体链路的连通性，测试结果均以数字显示。

无论是以太网、快速以太网，还是千兆位以太网，对线路的长度都做出了明确的规定。其中，以太网、快速以太网所允许的最大长度为 100m，千兆位以太网所允许的长度为 15m。使用 Fluke MircoScanner Pro 还可测量线缆的长度是否符合标准。

② 双绞线电气性能测试：对于规范的网络布线系统，应当分别对双绞线布线和光纤布线进行性能测试，以保证在连通性完好的同时，能够实现相应布线所能提供的带宽和数据传输速率。Fluke DTX 系列线缆认证分析仪（如图 7-27 所示）是一款既可满足当前要求又可面向未来技术发展的高技术测试平台，被广泛应用于网络布线系统的测试。


图 7-26　Fluke MicroScanner Pro

图 7-27　Fluke DTX 系列线缆认证分析仪

开始测试双绞线性能前，应当将 Fluke DTX 测试仪连接至要测试的网络链路中。需要注意的是，测试不同类型的链路应当使用不同的模块。测试双绞线水平布线链路时，Fluke DTX 测试仪的连接如图 7-28 所示。

③ 衰减测试与标准。衰减是信号在传输介质上进行传输的过程中所产生的损耗。

④ 近端串扰（NEXT）测试与标准。NEXT 是指在一条链路中从一对线至另一对线的信号耦合，也就是说当一条线对发送信号时在另一条相邻的线对收到的信号。近端串扰本身对终接点（跳线架、信息插座）处的非双绞金属线很敏感；同时，对粗劣的安装也非常敏感。NEXT 是决定链路传输能力的最重要的参数，在施工中的工艺问题也会产生 NEXT。

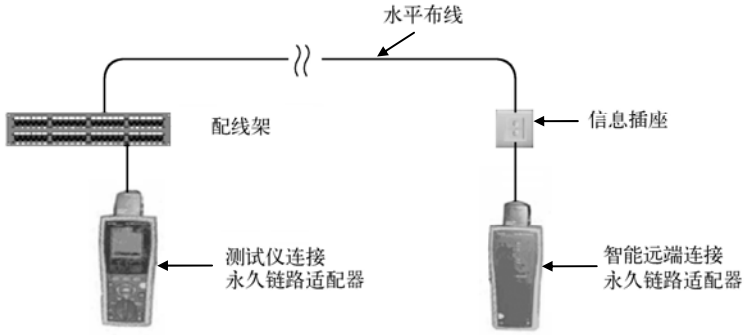



图 7-28　双绞线水平布线链路测试连接

Fluke DTX 广泛支持目前局域网布线中使用的各种屏蔽双绞线和非屏蔽双绞线（STP 、FTP、SSTP 和 UTP），并包含了许多由标准团体制定的测试限制（如 TIA、ISO、EN、Aus 和许多应用领域的专用测试限制），可以测试出当前所使用的双绞线类型、极限值、线缆的长度、所配置的线序等。Fluke DTX 还有一个值得称颂的功能，就是在非常短的时间内完成双绞线的自动测试（例如，可以在 12s 内完成一个 6 类双绞线网络的测试工作），并能完整准确地显示测试结果。另外，还可以在短时间内检测出网络中出现的故障位置。

**3．光纤链路测试**

光纤测试距离相对比较远，仪器也比较精密。Fluke DTX 同时可测试和诊断光纤网络，并且通过应用独家设计技术而大大提高测试速度。

测试光纤链路时，Fluke DTX 测试仪的连接如图 7-29 所示。

图 7-29　光纤链路测试仪的连接

Fluke DTX 测试仪可根据传输模式、波长等多种常用分类标准，来测试当前光纤的类型；Fluke DTX 的光纤测试模块通过双波长和双向测试速度提高了许多，仅需 12s 即可测试出输入光纤和输出光纤的损耗情况及长度等详细结果。

Fluke DTX 附带的光纤模块还集成了一个可视故障定位器（VFL），能够帮助用户快速检查光纤连通性、描记光纤曲线图，并找到光纤及连接器沿线上的故障问题，为故障排除带来很大帮助。

## 7.4.4　网络工程的测试与验收

网络工程的测试是对网络设备、网络系统及网络应用的支持设备进行检测，以证明网络系统能否满足用户在性能、安全性、易用性、可管理性等方面的需求。

**1．网络工程的测试**

网络工程测试包括网络设备测试、网络系统测试和网络应用测试 3 个内容。

（1）网络设备测试。网络设备测试主要包括设备功能测试、可靠性和稳定性测试、一致性测试、互操作性测试和性能测试。

① 功能测试。功能测试一般可依据产品说明书和相关说明资料对所具有的每项功能进行

逐一的测试。例如，针对网络防火墙说明书上对该产品端口和路由功能的说明等，对其端口进行的端口功能和路由功能的测试等。

② 可靠性和稳定性测试。往往通过加重设备负载的办法来分析和评估系统的可靠性和稳定性。例如，测试防火墙的可靠性和稳定性可以采用对其进行各种病毒攻击的方式，对经测得的数据进行详细整理和分析，得出该产品的抗攻击能力。

③ 一致性测试。一致性测试时测试验证产品的各项功能是否符合标准，如有些设备提供的端口标准是 100Mbps 数据传输率，但是实际情况未必能够达到。

④ 互操作性测试。所谓的互操作性也就是指设备的兼容性。因为所有的网络设备并非来自同一个厂家，而不同的厂家的产品不一定兼容，所以必须考察不同厂家的多种网络产品在互连的网络环境中是否能很好地工作。

⑤ 性能测试。性能测试的主要目的是分析产品在各种不同的配置和负载下的容量和对负载的处理能力。

典型的网络设备测试方法有两种：第一种是将设备放在一个仿真的网络环境中进行测试；第二种是使用专用的网络测试设备对产品进行测试。用户可以根据自己的实际情况选择合适的测试方式。

（2）网络系统测试。网络系统的测试包括网路系统的规划验证测试、性能测试、可靠性与可用性的测试，以及评估、网络流量和模型化测试等，通过对网络系统的主动测量和被动检测确定系统中站点的可达性、网络系统的吞吐量、传输速率、带宽利用率、丢包率、服务器和网络设备的相应时间、具体应用和用户产生最大的网络资源，以及服务质量等。网络系统测试的核心工具是协议分析仪。

（3）网络应用测试，主要是测试网络对各种服务和应用的支持水平，是从实际应用的角度对网络性能的验证。

### 2．网络工程的验收

对网络工程验收是施工方（乙方）向用户方（甲方）移交的正式手续，也是用户对工程的认可。作为验收，是分两部分进行的，第一部分是物理验收；第二部分是文档与系统测试验收。

（1）现场（物理）验收。甲方、乙方共同组成一个验收小组，对已竣工的工程进行验收。作为网络综合布线系统，在物理上的主要验收点是：

① 施工过程中甲方需要检查的事项。

- 环境要求；
- 施工材料的检查；
- 安全、防火要求。

② 检查设备安装。

- 机柜与配线面板的安装；
- 网络设备的安装；
- 信息模块的安装。

③ 双绞线电缆和光纤安装。

- 桥架和线槽安装；

- 线缆布放。

④ 室外光纤的布线。

- 架空布线；
- 管道布线；
- 挖沟布线（直埋）；
- 隧道线缆布线。

⑤ 线缆终端安装。上述 5 点均应在施工过程中由甲方和督导人员随工检查。发现不合格的地方，做到随时返工，如果完工后再检查，出现问题就不好处理了。

（2）文档与系统测试验收。文档验收主要是检查乙方是否按协议或合同规定的要求，交付所需要的文档。系统测试验收就是由甲方组织的专家组，对信息点进行有选择的测试，检验测试结果。

需测试的内容主要有：

- 电缆的性能测试；
- 光纤的性能测试；
- 系统接地要求测试。

乙方要准备的文档资料有：

- 网络综合布线工程建设报告；
- 网络综合布线工程测试报告；
- 网络综合布线工程资料审查报告；
- 网络综合布线工程用户意见报告；
- 网络综合布线工程验收报告。

# 练习 7

**一、填空题**

（1）网络规划的目的是通过科学合理的规划，能够取得用_____的成本建立_____的网络，达到较高的性能，提供最优的服务的完美效果。

（2）网络规划需要进行的主要工作包括：网络_____分析、网络_____分析、网络扩展性分析。

（3）网络规模与结构分析包括确定网络规模、_____分析、与外部_____方案等。

（4）通常网络拓扑设计的分层结构可包括 3 个层次，即_____层、_____层和接入层。

（5）接入层的设计目标包括 3 个方面，即_____馈入、_____访问、广播限制。

（6）综合布线系统可以划分成 6 个子系统，即工作区（终端）子系统、_____子系统、管理间子系统、_____子系统、设备间子系统、建筑群子系统。

（7）水平布线子系统一般使用_____线缆，最大水平距离为_____米。

（8）对网络工程验收是施工方向用户方移交的正式手续，也是用户对工程的认可。验收分两部分进行，第一部分是_____验收；第二部分是_____验收。

## 二、选择题

（1）网络中某一台设备或某一条链接发生故障就能导致整个网络瘫痪，发生这种故障的设备节点或链路被称为（　　）。

A．单故障点　　B．多故障点

C．故障集合点　　D．故障链路

（2）在分布层提供冗余的两种最普通的方法是（　　）和“到其他分布层路由器的备份链接”。

A．双向　　B．双归　　C．多路　　D．聚合

（3）地址分配的一般原则是（　　）。

A．使用尽可能大的地址空间　　B．留下一定空间以供将来扩展

C．尽可能减小地址开销　　D．以上都对

（4）T568B 标准描述的线序为（　　）。

A．1—白绿、2—绿、3—白橙、4—蓝、5—白蓝、6—橙、7—白棕、8—棕

B．1—白橙、2—橙、3—白绿、4—蓝、5—白蓝、6—绿、7—白棕、8—棕

C．1—白绿、2—橙、3—白橙、4—蓝、5—白蓝、6—绿、7—白棕、8—棕

D．1—白棕、2—棕、3—白绿、4—蓝、5—白蓝、6—绿、7—白橙、8—橙

（5）无论是以太网、快速以太网，还是千兆位以太网，对线路的长度都做出了明确的规定。其中，快速以太网和千兆位以太网所允许的双绞线长度为（　　）。

A．90m，50m　　B．90m，15m

C．100m，15m　　D．100m，50m

# 第 8 章

# 网络管理与安全

随着网络的迅速发展，如何管理当前网络和网络的安全性显得非常重要，这是因为怀有恶意的攻击者窃取、修改网络上传输的信息，通过网络非法进入远程主机，获取存储在主机上的机密信息，或占用网络资源，阻止其他用户使用等，而且目前网络技术日新月异，网络的复杂性在不断增长，对网络管理的要求也日益增加。然而，网络作为开放的信息系统必然存在众多潜在的安全隐患，因此，网络安全与管理作为一个独特的领域越来越受到关注。

通过本章的学习，应达到如下的学习目标：

（1）熟悉网络管理的功能，了解常用的网络故障诊断方法；

（2）了解网络安全的概念及网络所面临的主要威胁；

（3）熟悉常用的网络安全机制；

（4）熟悉防火墙的功能、分类及应用。

## 8.1 网络管理基础

### 8.1.1 网络管理概述

随着网络技术的发展，网络的组成日益复杂，多厂商、异构网、跨技术领域的复杂网络环境，对网络管理的要求也越来越高。但由于网络应用环境、管理制度和文化背景的不同，造成管理需求的差异很大。任何供应厂商都难以提供一个完整的解决方案，尤其是对于各种新的网络技术，仍需要有自己的专家和工程师进行管理和维护。20 世纪 80 年代以来，网络的增长速度很快，不同类型的网络设备骤增，因此能够管理各类异构网络，并能在不同的环境中自动进行网络管理与规划，成为一种新的迫切需求。

#### 1．网络管理的目的和内容

（1）网络管理的目的。

网络管理，简单地说就是为了保证网络系统能够持续、稳定、高效和可靠地运行，对组成网络的各种软、硬件设施和人员进行的综合管理。网络管理的任务就是收集、分析和检测监控网络中各种设备、设施的工作参数和工作状态信息，将结果显示给网络管理员并进行处理，从而控制网络中设备、设施的工作参数和工作状态，以实现对网络的管理。

（2）网络管理的基本内容。

① 数据通信网中的流量控制。网络的吞吐量是有限的，当在网络中传输的数据量超过网络容量时，网络中就会发生阻塞，严重时会导致网络系统瘫痪。因此，流量控制是网络管理的重要内容。

② 路由选择策略管理。网络的路由选择方法不仅应具有正确、稳定、最佳和简捷等特点，还应能够适应网络规模、网络拓扑和网络中数据流量的变化。因为在网络系统中，数据流量总是不断变化的，网络拓扑也可能发生变化，为此，系统应始终保持所采用的是最佳的路由选择方案。所以，网络管理必须要有一套管理方法和提供路由管理的机制。

③ 网络安全保护。计算机网络系统给人们带来的最大方便是用户之间可以非常容易地实现充分的网络资源共享，但网络系统中共享的资源具有完全开放、部分开放和不开放等区别，从而出现系统资源的共享与保护之间的矛盾。为了解决这个矛盾，在网络中要引入安全机制。其目的就是用来保护网络用户信息不被侵犯、网络资源不被破坏和网络不被非法入侵等。

④ 网络的故障诊断与修复。由于网络系统在运行过程中不可避免地会发生故障，而准确、及时地确定故障位置和产生原因是解决故障的关键。对网络系统实施强有力的故障诊断是及时发现系统隐患、保证系统正常运行所必不可少的。一旦网络故障被诊断出来，故障原因也找到了，就可以对症下药，进行故障修复。

此外，网络管理的内容还涉及用户管理、网络状态检测、设备维护和管理、网络规划、网络资产管理等。

### 8.1.2 网络管理的功能

网络管理功能是为网络管理员进行监视、控制和维护网络而设计的。在 OSI 管理标准中，将系统管理功能分为故障管理、配置管理、计费管理、性能管理和安全管理。这 5 种管理功能只是网络管理的基本功能，诸如网络规划、数据库管理、操作人员管理等均未包括在内。

（1）故障管理（Fault Management）。故障管理是最基本的网络管理功能。

故障管理是指对故障的检测、诊断、排除或恢复等操作进行管理。其目的是保证为网络提供连续、可靠的服务。故障管理接收故障报告，发起纠正动作。但纠正动作一般是通过配置管理设施或操作员干预来实现的。故障管理的内容包括检测被管理对象的差错、接收差错通知；利用空余设备或迂回路由，提供新的网络资源用于服务；差错日志库的创建与维护；对差错日志进行分析；检测到差错后应采取的动作；进行诊断、测试，以便跟踪和识别故障等。

（2）配置管理（Configuration Management）。配置管理也是基本的网络管理功能。

随着用户数的增加、设备的故障与维修等，计算机网络的配置经常发生变化，这些变化无论是暂时性的还是永久性的，都要求网络管理系统必须有足够的技术支持这些变化。配置管理就是用来定义、鉴别、初始化、控制和检测通信网中的被管理对象的功能集合。具体内容有：

- 鉴别所有被管理对象，给每个被管理对象分配名字；
- 定义新的被管理对象，删除不需要的被管理对象；
- 设置被管理对象的初始值；

- 处理被管理对象之间的关系；
- 改变被管理对象的操作特性；
- 报告被管理对象的状态变化。

（3）计费管理（Accounting Management）。

计费管理是自动记录用户使用网络资源和时间的情况，提供收缴费用的原始数据。用户使用网络资源的计费办法有多种，如主叫付费和被叫付费，或主叫和被叫分担费用。不同的资源收费标准也不一样，不同的用户对服务的要求也不同。要让用户根据自己的需要和费用选择适当的服务，这要有自动化管理系统的支持。如通用网络计费系统（CNGAS）能够实现上述功能，而且配置灵活，适应性强，操作非常简便。

（4）性能管理（Performance Management）。

性能管理活动是持续地检测网络运行中的主要性能指标，以检验网络服务是否达到预定的水平，找出潜在的或已经发生的不利因素，报告网络性能的变化趋势，为网络管理决策提供依据。为了达到这些目的，网络性能管理功能需要维护性能数据库，需要与性能管理功能域保持联系，并自动地完成网络管理。性能管理的具体内容包括：

- 从被管理对象中收集网络性能参数、记录和维护历史数据；
- 对当前数据进行统计、分析，检测性能故障，产生性能告警和报告性能事件；
- 将当前数据统计分析结果与历史模型进行比较，做趋势预测；
- 形成和改进网络性能评价准则，以性能管理为目标，改进网络操作模式。

（5）安全管理（Security Management）。

网络安全管理的目标是防止用户对网络资源的非法访问，确保网络资源和网络用户的安全。安全管理的主要内容有：

- 分发与安全措施有关的信息，如密钥的分发、访问优先权的设置等；
- 发出与安全有关事件的通知，如网络有非法侵入、无权用户企图访问特定信息等；
- 创建、控制和删除与安全有关的服务和设施；
- 记录、维护和查阅安全日志，以便对安全进行追踪等事后分析。

### 8.1.3　简单网络管理协议

由于历史和现实的原因，国际标准化组织 ISO 制定的网络管理标准——公共管理信息服务 CMIS 和公共管理信息协议 CMIP，与 ISO 的开放系统互联参考模型标准一样，通常在电信网（如 SDH）中得到应用，在局域网中始终未得到用户（厂商）的广泛支持。相反，广泛应用于 TCP/IP 网络的简单网络管理协议（SNMP）却得到所有网络厂商的一致支持。

#### 1．SNMP 模型

SNMP 是（Simple Network Management Protocol）的缩写，它的中文意思是简单网络管理协议。是一个应用层网络协议。该协议设计的主要目的是为网络设备之间提供管理信息交换的设施。采用 SNMP 协议访问网络管理信息，网络管理人员可以更加容易地管理网络，发现和解决网络问题。SNMP 的优点是协议简单，易于实现；缺点是管理通信开销大。

SNMP 模型如图 8-1 所示。该模型组成的 4 个要素是：网络管理站（管理进程）、被管理

者（管理代理）、管理信息库（MIB）和网络管理协议（SNMP）。

（1）网络管理站。网络管理站是指具有运行网络管理协议 SNMP 和运行网络管理支持工具及网络管理应用软件的主机。网络中至少有一台这样的主机，它运行特殊的网络管理软件（管理进程）。管理进程完成各种网络管理功能，通过各设备中的管理代理对网络中的各种设备、设施和资源实施检测和控制。另外，操作人员通过管理进程对全网进行管理。有时管理进程也会对各管理代理中的数据集中存档，以备事后分析。

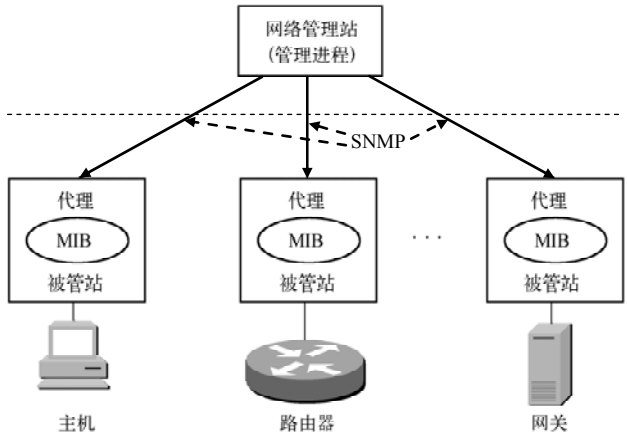



图 8-1　SNMP 模型

（2）被管理站。被管理者（管理代理 Agent）包括主机、网关、服务器、路由器、交换机等网络设备。管理代理是驻留在被管设备上的一套软件，它负责执行管理进程的管理操作。管理代理直接操作本地信息库 MIB，如果管理进程需要，它可根据要求改变本地 MIB 或通过本地 MIB 提取数据并传回到管理进程。每个管理代理都有自己的本地 MIB。一个代理管理的本地 MIB 不一定具有 Internet 定义的 MIB 的全部内容，而只需要包括与本地设备或设施有关的管理对象。管理代理可以从 MIB 中读取各种变量值，也可以在 MIB 中修改各种变量值，并可以与管理进程进行通信，以响应其管理请求。

（3）管理信息库 MIB。MIB 是一个概念上的数据库，由管理对象组成。每个管理代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。MIB 包括报文分组计数、出错计数、用户访问计数、路由器中的 IP 路由选择表等。MIB 分为 MIB Ⅰ（通用管理信息库）和 MIB Ⅱ（专用管理信息库）两类，后者由各厂商自行定义。

（4）SNMP 协议。SNMP 协议最重要的特性就是简捷易用，从而使系统的负载减至最低限度。SNMP 中没有一大堆命令，而只有存（存储数据到变量集）和取（从变量集中取数据）两种操作。在 SNMP 中，所有操作都可以看成是由这两种操作派生而来的。正是由于这些特性，使得 SNMP 的开发非常方便，成为网络管理事实上的标准。

在 SNMP 中，只定义了 4 种操作：① 取（get），从管理代理那里取得指定的 MIB 变量值；② 取下一个（get next），从管理代理表中取得下一个指定的 MIB 值；③ 设置（set），设置管理代理指定的 MIB 变量值；④ 报警（trap），当管理代理发现被管对象出现严重错误时，立即向网络管理站报警，无须等待接收方响应。

相应的，SNMP 协议有如下 4 种基本协议交互过程：

① 管理进程从管理代理那里获取管理信息，即管理进程向管理代理发送 get-request 后，

管理代理向管理进程返回相应的管理信息 get-response；

② 管理进程向管理代理发送 get-next-request，管理代理返回 get-response，将在前次访问基础上的下一管理对象的值返回给管理进程；

③ 管理进程向管理代理发送 set-request，对管理代理的 MIB 进行写操作，由管理代理完成 set 操作，管理代理用 set-response 返回操作结果；

④ 管理代理使用 trap 向管理进程报告紧急事件，无须响应。

2．SNMPv2

前面介绍的 SNMP（称为 SNMPvl）的优点是简单、便捷，因此得到了广泛应用。但它还存在着如不能有效地传输大块数据，不能将网络管理功能分散化，安全性能不够理想等缺点。

1996 年推出的 SNMPv2 能够克服上述缺点，但在安全性方面仍未取得突破性进展。SNMPv2 增加了一个叫做 get-bulk-request 的命令，可一次从路由器的路由表中读取多行信息，而不像 SNMPvl 那样，一次只读一行信息；SNMPv2 的另一个特点是改进了原来的 get 命令。SNMPvl 在使用 get 命令读取多个变量的信息时，只要有一个变量值不能返回，整个的 get 命令就被拒绝。因此管理进程就减少了变量数目，要重新发送 get 命令。SNMPv2 的 get 命令允许返回部分的变量值，这样可提高效率，减少网上通信量。

当网络规模扩大时，使用一个网络管理站对全网集中管理是不合适的。SNMPv2 采用了较好地分散化管理方法。在一个网络中可以有多个顶级管理站（管理服务器），每个这样的管理服务器管理网络的一部分代理进程，并指派若干个代理进程使之具有管理其他代理进程的功能。这种结构分散了处理功能，使得网络总的通信量明显降低。为了支持这种配置，SNMPv2 增加了 inform 命令和一个管理进程到管理进程的 MIB。使用这种 inform 命令可以使管理进程之间互相传输有关的信息而无须经过请求。这样的信息则定义在管理进程到管理进程的 MIB 中。

### 8.1.4　网络故障诊断

网络中可能出现的故障多种多样，往往解决一个复杂的网络故障需要广泛的网络知识与丰富的工作经验。这也是为什么一个成熟的网络管理机构，需要有一整套完备的故障管理日志记录机制，另外，由于网络故障的多样性和复杂性，网络故障的解决方法也不尽相同。

网络故障诊断应该实现如下 3 方面的功能：

- 确定网络的故障点，恢复网络的正常运行；
- 发现网络规划和配置中欠佳之处，改善和优化网络的性能；
- 观察网络的运行状况，及时预测网络通信质量。

网络故障诊断以网络原理、网络配置和网络运行的知识为基础。从故障现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源，排除故障，恢复网络正常运行。网络故障通常有以下几种可能：物理层中物理设备相互连接失败或者硬件及线路本身的问题；数据链路层网络设备的接口配置问题；网络层网络协议配置或操作错误；传输层的设备性能或通信拥塞问题；上三层或网络应用程序错误。诊断网络故障的过程应该沿着 OSI 七层参考模型从物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类

推，设法确定通信失败的故障点，直到系统通信正常为止。

网络诊断可以使用包括局域网或广域网分析仪在内的多种工具，如路由器诊断命令；网络管理工具和其他故障诊断工具。CISCO 提供的工具足以胜任排除绝大多数网络故障。查看路由表，是解决网络故障开始的好地方。ICMP 的 ping、trace 命令和 Cisco 的 show 命令、debug 命令等是获取故障诊断有用信息的重要工具。通常使用一个或多个命令收集相应的信息，在给定情况下，确定使用什么命令获取所需要的信息。譬如，通过 IP 协议来测定设备是否可将信息正确传送的常用方法是使用 ping 命令。ping 从源点向目标发出 ICMP 信息包，如果成功的话，返回的 ping 信息包就证实从源点到目标之间所有物理层、数据链路层和网络层的功能都运行正常。如何在互联网络运行后了解网络运行是否正常？监视和了解网络在正常条件下的运行细节？了解出现故障的情况？利用 show interface 命令可以非常容易地获得待检查的每个接口的信息。另外 show buffer 命令提供定期显示缓冲区大小、用途及使用状况等。show proc 命令和 show proc mem 命令可用于跟踪处理器和内存的使用情况，可以定期收集这些数据，在故障出现时，用于诊断参考。 网络故障以某种症状表现出来，故障症状包括一般性的（如用户不能接入某个服务器）和较特殊的（如路由器不在路由表中）。对每一个症状使用特定的故障诊断工具和方法都能查找出一个或多个故障原因。

一般故障排除步骤如下：第一步，当分析网络故障时，首先要清楚故障现象。应该详细说明故障的症候和潜在的原因。为此，要确定故障的具体现象，然后确定造成这种故障现象的原因。例如，主机不响应客户请求服务。可能的故障原因是主机配置问题、接口卡故障或路由器配置命令丢失等。第二步，收集需要的用于帮助隔离可能故障原因的信息。向用户、网络管理员、管理者和其他关键人物提一些和故障有关的问题。广泛的从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。第三步，根据收集到的情况考虑可能的故障原因。可以根据有关情况排除某些故障原因。例如，根据某些资料可以排除硬件故障，把注意力放在软件原因上。对于任何机会都应该设法减少可能的故障原因，以至于尽快地策划出有效地故障诊断计划。第四步，根据最后确定的可能的故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样可以容易恢复到故障的原始状态。如果一次同时考虑一个以上的故障原因，试图返回故障原始状态就困难得多了。第五步，执行诊断计划，认真做好每一步测试和观察，直到故障症状消失。第六步，每改变一个参数都要确认其结果。分析结果确定问题是否解决，如果没有解决，继续下去，直到解决。

### 8.1.5 常用网络诊断工具

很多网络管理工具都集成到网络操作系统中，单独的网络管理工具不多，但仍然有简单、实用的网络管理工具，这些工具包括连通性测试程序（ping）、网络协议统计工具（Netstat）、网络跟踪工具（Tracert）、测试 TCP/IP 配置工具 Ipconfig/winipcfg 等。

#### 1．连通性测试程序（ping）

ping 是 Windows 系统中集成的一个专用于 TCP/IP 协议网络中的测试工具，ping 命令用于查看网络上的主机是否在工作，它是通过向该主机发送 ICMP ECHO_REQUEST 包进行测试而达到目的的。一般凡是使用 TCP/IP 协议的网络，当发生计算机之间无法访问或网络工作

不稳定时，都可以试用 ping 命令来确定问题的所在。

ping 命令是将 ICMP ECHO_REQUEST 包发送给指定的计算机，如果 ping 成功了，则 TCP/IP 把 ICMP ECHO_REQUEST 包发送回来，其发回的结果表示能否到达主机、向主机发送一个返回数据包需要多长时间等。使用 ping 可以确定 TCP/IP 配置是否正确以及本地计算机与远程计算机是否正在通信。

在局域网的维护中，经常使用 ping 命令来测试网络是否通畅。使用 ping 命令检查局域网上计算机的工作状态的前提条件是：局域网计算机必须已经安装了 TCP/IP 协议，并且每台计算机已经配置了固定的 IP 地址。应用 ping 命令操作步骤如下：

（1）在 MS-DOS 提示符下，输入 ping 测试的目标计算机的 IP 地址或主机名，如要测试一台 IP 地址为 192.168.1.10 的客户机与服务器是否已经联网，可以在局域网中任意一台计算机的 DOS 界面下运行 ping 192.168.1.10。

（2）命令执行后，如果客户机上的 TCP/IP 协议工作正常，则会以 DOS 屏幕方式显示类似的“Reply from IP 地址：bytes=32 time<1ms TTL=128”信息，如图 8-2 所示。

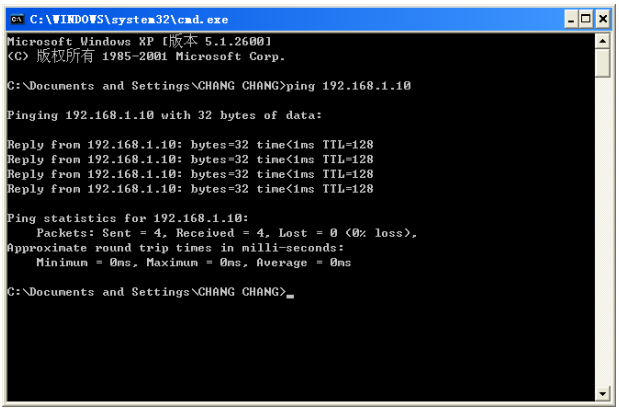



图 8-2　ping 192.168.1.10 成功信息

（3）如果网络未连接成功，则显示“Request Time out 或 Destination host unreachable（请求超时）”信息，如图 8-3 所示。

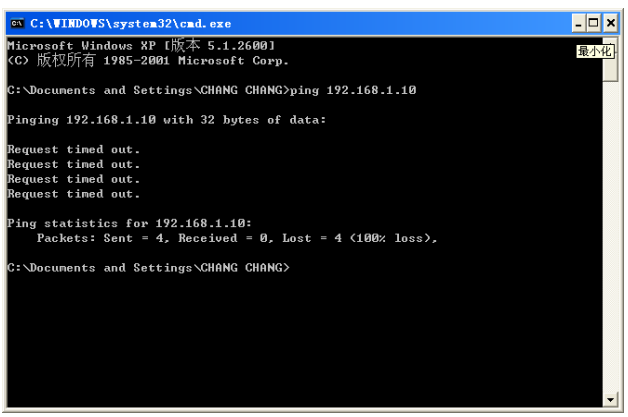



图 8-3　连接失败信息

出现以上错误提示的情况时，就要仔细分析一下网络故障出现的原因和可能有问题的网

上节点了。可以从协议方面来着手检查。网卡是否安装正确，IP 地址是否被其他用户占用。检查本机和被测试的计算机的网卡及交换机（集线器）指示灯是否为亮，来判断是否已经连入整个网络中。是否已经安装了 TCP/IP 协议，TCP/IP 协议的配置是否正常。检查网卡的 I/O 地址、IRQ 值和 DMA 值，是否与其他设备发生冲突。如果还是无法解决，建议用户重新安装和配置 TCP/IP 协议。

在使用 ping 命令进行故障诊断时，可以通过 ping 下列地址来判断故障的位置：

（1）ping 127.0.0.1：在此命令执行时，计算机将模拟远程操作的方式来检测本机，如果不通，则极有可能是 TCP/IP 协议安装不正确，应删除 TCP/IP 协议，重新启动计算机，再重新安装 TCP/IP 协议；或者网络适配器安装有问题，应删除后重新添加。

（2）ping 本机 IP 地址不通，则说明在相应端口上的协议绑定有问题，查看网络设置，可能是网络协议绑定不正确。

（3）ping 其他主机 IP 地址：如果前两种方式都能 ping 通，而不能 ping 其他主机的 IP 地址，那么说明其他主机的网络设置有问题，或者网络连接有问题，可以检查其他主机的网络设置，检查物理连接是否有问题。

### 2．网络协议统计工具（Netstat）

Netstat 命令是运行于 DOS 界面下，利用该工具可以显示有关统计信息和当前 TCP/IP 网络连接的情况，用户或网络管理人员可以得到非常详尽的统计结果。当网络中没有安装特殊的网管软件，但要对整个网络的使用状况做个详细的了解时，就是 Netstat 大显身手的时候了。

Netstat 命令可用来获得当前系统网络连接的信息、收到和发出的数据、被连接的远程系统端口等。

Netstat 的应用主要有以下几个方面：

（1）了解本地与之相连的远程计算机的连接状态，包括 TCP、IP、UDP、ICMP 协议的使用情况，了解本地机器开放的端口情况。

（2）检查网络接口是否已经正确安装，如果在用 Netstat 命令后仍不能显示某些网络接口的信息，则说明这个网络接口没有正确连接，需要重新查找原因。

（3）通过加入“-R”参数查询与本机相连的路由器分配情况，如图 8-4 所示。

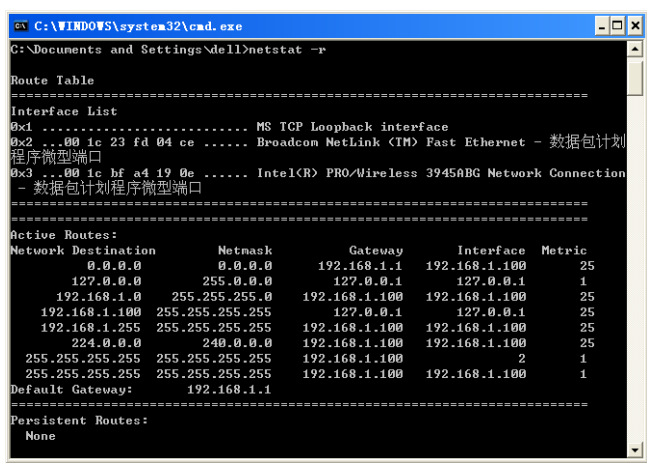



图 8-4　查询分配情况

3．测试 TCP/IP 配置工具 Ipconfig/winipcfg

利用 Ipconfig 工具可以查看和修改网络中的 TCP/IP 协议的有关配置，如 IP 地址、网关、子网掩码等。Ipconfig 这个工具以 DOS 提示符的形式显示。通过以上各种系统自带的工具，用户可以轻松地查看网络协议的配置及网络环境的状态，为更好地分析和诊断网络故障提供了很好的帮助。当诊断出网络故障中的问题后就可以对症下药了。

# 8.2　网络安全

随着计算机网络的发展，尤其是 Internet 的普及，计算机的应用更加广泛与深入，同时计算机系统的安全问题日益突出和复杂。一方面，网络系统提供了资源的共享性，提高了系统的可靠性，通过分散工作负荷提高了工作效率，并具有可扩充性。这些特点使得计算机网络应用深入到国民经济、国防、科技、教育等各个领域；另一方面，也正是这些特点，增加了网络系统的脆弱性和网络安全的复杂性，增加了网络受威胁和攻击的可能性。事实上，资源共享和信息安全是一对矛盾，随着资源共享的加强，网络安全的问题也日益突出。据报道，美国每年因网络安全问题所造成的经济损失高达近百亿美元，而全球每 20s 就发生一起 Internet 不安全事件。

## 8.2.1　网络安全概述

1．网络安全的概念

“网络安全”可理解为“网络系统不存在任何威胁状态”，即为防范诸如病毒的破坏、黑客的入侵、计算机犯罪、人为的主动或被动攻击等威胁，而采取一些措施则可保证网络系统的相对安全。

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏和泄露。具体地说，网络安全是指通过采取各种技术和管理措施，使网络系统的硬件、软件及其系统中的数据资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄露，保证网络系统连续、可靠、正常地运行。

网络系统的安全主要涉及系统的可靠性、软件和数据的完整性、可用性和保密性几方面的问题。因此，网络系统的安全性的含义可包括系统的可靠性、软件和数据的完整性、可用性和保密性等几个特征。

- 网络系统的可靠性：是指保证网络系统不因各种因素的影响而中断正常工作；
- 软件和数据的完整性：是指保护网络系统中存储和传输的软件（程序）与数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序，数据库中的数据或系统中的程序不被破坏等；
- 软件和数据的可用性：是指在保证软件和数据完整的同时，还要能使其被正常利用和操作；

- 软件和数据的保密性：主要是利用密码技术对软件和数据进行加密处理，保证在系统中存储和网络上传输的软件和数据不被无关人员识别。

**2．网络安全级别**

美国国防部开发的计算机安全标准《可信计算机系统标准评价准则》将安全级别分为四类七级：

- D1 级（安全的最低级）：该级不设置任何安全保护措施，软、硬件都容易被侵袭。MS-DOS、Windows 95/98 等系统为 D1 级（缺乏保护）；
- C1 级（选择性安全保护级）：硬件采取简单安全措施（加锁），登录认证和访问权限不能控制已登录用户的访问级别。早期的 UNIX/Xenix、NetWare 3.x 等属于该级；
- C2 级（访问控制环境级）：比 C1 级增加了系统审计、跟踪记录、安全事件等特性。UNIX、NetWare 4.x 及以上版、Windows NT 等属于该级，C2 级是保证敏感信息安全的最低级；
- B1 级（标记安全保护级）：B1 级系统拥有者为政府机构和防御承包商；
- B2 级：结构化安全级（Structured Protection）；
- B3 级：安全域级（Security Domain）；
- A1 级：验证设计级（Verity Design），最高安全级。

## 8.2.2 网络安全的主要威胁

影响网络系统安全的威胁主要来自于网络系统的脆弱性、利用网络协议和系统漏洞的一些行为及计算机病毒 3 个方面。

**1．网络系统的脆弱性**

计算机网络本身存在着一些固有的弱点（如脆弱性），非授权用户利用这些脆弱性可对网络系统进行非法访问，这种非法访问会使系统内数据的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是可被窃取有价值的信息而不留任何痕迹。

网络系统的脆弱性主要表现在以下几个方面：

- 操作系统的脆弱性：网络操作系统体系结构本身就是不安全的——操作系统程序具有动态连接性；操作系统可以创建进程，这些进程可在远程节点上创建与激活，被创建的进程可以继续创建其他进程;NOS 为维护方便而预留的无口令入口也是黑客的通道。
- 计算机系统本身的脆弱性：主要表现为硬盘故障、电源故障、主板芯片故障、操作系统和应用软件故障；另外若存在超级用户，而入侵者得到了超级用户口令，整个系统将完全受控于入侵者。
- 电磁泄漏：网络端口、传输线路和处理机都有可能因屏蔽不严或未加屏蔽而造成电磁信息辐射，从而造成信息泄露。
- 数据的可访问性：数据可容易地被复制而不留任何痕迹；网络用户在一定的条件下，可以访问系统中的所有数据，并可将其复制、删除或破坏掉。
- 通信系统和通信协议的弱点：网络系统的通信线路面对各种威胁就显得非常脆弱，非

法用户可对线路进行物理破坏、搭线窃听、通过未保护的外部线路访问系统内部信息等；TCP/IP 中的 FTP、E-mail、NFS、WWW 等都存在安全漏洞，如 FTP 的匿名服务浪费系统资源，E-mail 中潜伏着电子炸弹、病毒等威胁互联网安全，WWW 中使用的通用网关接口程序、Java Applet 程序等都能成为黑客的工具，黑客可采用 Sock、TCP 预测、远程访问或直接扫描等手段攻击防火墙。

- 数据库系统的脆弱性：由于数据库管理系统（DBMS）对数据库的管理是建立在分级管理的概念上，因此，DBMS 的安全性也是可想而知的；DBMS 的安全必须与操作系统的安全配套，这无疑是一个先天的不足之处；黑客通过探访工具可强行登录和越权使用数据库资源；数据加密往往与 DBMS 的功能发生冲突或影响数据库的运行效率。
- 网络存储介质的脆弱性：软、硬盘中存储大量的信息，这些存储介质很容易被盗窃或损坏，造成信息的丢失。

此外，网络系统的脆弱性还表现为保密的困难性、介质的剩磁效应和信息的聚生性等。

### 2．利用网络协议和系统漏洞的一些威胁行为

利用网络协议和系统漏洞的一些威胁行为主要表现有：非法授权访问、假冒合法用户、病毒破坏、线路窃听、干扰系统正常运行、修改或删除数据等。这些威胁大致可分为无意威胁和故意威胁两大类。

- 无意威胁：是在无预谋的情况下破坏了系统的安全性、可靠性或资源的完整性等。无意威胁主要是由一些偶然因素引起的，如软、硬件的机能失常，不可避免的人为错误，电源故障和自然灾害等；
- 故意威胁：实际上就是“人为攻击”。由于网络本身存在脆弱性，因此总有某些人或某些组织想方设法利用网络系统达到某种目的，如从事工业、商业或军事情报搜集工作的间谍，对相应领域的网络信息是最感兴趣的，他们构成了网络系统安全的主要威胁。

攻击者对系统的攻击范围，可从随便浏览信息到使用特殊技术对系统进行攻击，以便得到有针对性的信息。这些攻击又可分为被动攻击和主动攻击。

被动攻击是指攻击者只通过观察网络线路上的信息，而不干扰信息的正常流动，如被动地搭线窃听或非授权地阅读信息。主动攻击是指攻击者对传输中的信息或存储的信息进行各种非法处理，有选择地更改、插入、延迟、删除或复制这些信息。这两种攻击可用图 8-5 形象地描述。

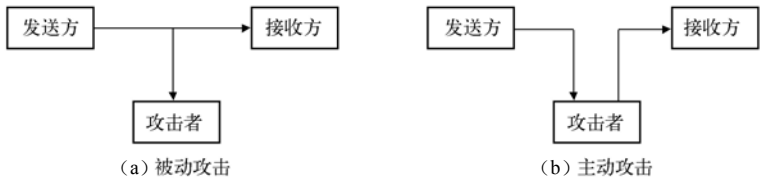



图 8-5　被动攻击和主动攻击

### 3．计算机病毒

随着计算机病毒的复杂化，病毒的防护越来越困难，其危害也越来越大。目前，成千上万种不同的病毒不时地对计算机和网络的安全构成严重威胁。因此，了解和控制病毒威胁的

需求显得格外的重要。

在我国正式颁布实施的《中华人民共和国计算机信息系统安全保护条例》第 28 条明确指出："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"这个定义具有法律性和权威性。

计算机病毒是一种能破坏计算机系统资源的特殊计算机程序。它像生物病毒一样，可在系统中生存、繁殖和传播。计算机病毒具有非授权可执行性、隐蔽性、传播性、潜伏性、可触发性、针对性、与黑客技术的结合性和破坏性等特征。它一旦发作，轻者会影响系统的工作效率，占用系统资源，重者会毁坏系统的重要信息，甚至使整个网络系统陷于瘫痪。在国际上，由于计算机病毒侵入网络而造成巨大损失的例子不胜枚举。

因此，计算机病毒的防护工作应成为保证网络系统安全性的一项重要内容。对计算机病毒要以预防为主，采取消除传染源、切断传染途径，保护易感染源等措施，增强网络系统对计算机病毒的识别和抵抗力。

随着 Internet 技术的发展，计算机病毒的含义也在逐步发生着变化，与计算机病毒特征和危害有类似之处的"特洛伊木马"和"蠕虫"，从广义角度而言也可归为计算机病毒之列。特洛伊木马通常又称为黑客程序，其关键是采用隐藏机制执行非授权功能。蠕虫通过网络来扩散和传播特定的信息或错误，进而造成网络服务遭到拒绝，并出现死锁现象或使系统崩溃。木马和蠕虫病毒对网络系统的危害日益严重。

一般意义上的计算机病毒是在 1986 年前后出现的。在此后的十多年时间里，病毒制作技术也从逐步发展到迅速发展，特别是进入 21 世纪的几年中，计算机病毒的发展非常快，病毒数量猛增，破坏性也越来越大。据预计，到目前计算机病毒的数量超过 10 万种。

计算机病毒因为其具有不同的特征，可能会同时属于多个不同类型。按照对系统的破坏程度的强弱不同，计算机病毒可分为良性病毒和恶性病毒；根据计算机病毒攻击的对象不同，可以分为攻击微型计算机的病毒、攻击小型计算机的病毒、攻击大中型计算机的病毒、攻击计算机网络的病毒等；根据计算机攻击计算机操作系统的不同，可以分为攻击 Macintosh 系统病毒、攻击 DOS 系统的病毒、攻击 Windows 系统的病毒、攻击 UNIX/Linux 系统的病毒、攻击 Netware 系统的病毒等；根据病毒链接方式不同，可以分为操作系统型病毒、外壳型病毒、嵌入型病毒、源码型病毒等；根据计算机语素传播方式的不同，可以分为文件传染源病毒、引导扇区病毒、主引导记录病毒、复合型病毒、宏病毒等。

## 8.3 网络安全机制

### 8.3.1 加密技术

加密是提供信息保密的核心方法。加密算法除了提供信息的保密性之外，它和其他技术结合，还能提供信息的完整性。因此加密的目的是防止机密信息的泄露，同时还可以用于证实信息源的真实性，验证所接收到的数据的完整性。

加密技术不仅应用于数据通信和存储，也应用于程序的运行，通过对程序的运行实行加密保护，可以防止软件被非法复制，防止软件的安全机制被破坏，这就是软件加密技术。

按密码体制的不同，加密算法有序列密码算法和分组密码算法之分。

### 1．序列密码算法

序列密码（也称为流密码）的思想是将明文序列与密钥流序列逐位异或得到密文。其主要优点是产生流密钥序列简单、加密与解密过程均不需复杂的算法、易于硬件实现、加/解密速度快。由于序列密码还具有扰乱明文统计特性、不存在数据扩展和误差传递等特点，非常适合于保密通信。序列密码在实际应用，特别是在军事、外交及重要机密文件发送中保持着独特的优势，成为当前军事和外交系统中应用的主流。

### 2．分组密码算法（DES）

DES（Data Encryption Standard）是目前研究最深入、应用最广泛的一种分组密码。是由 IBM 公司在 1971 年设计的一个加密算法。1977 年由美国国家标准局（现美国国家标准技术委员会）作为第 46 号联邦信息处理标准而采用的一种数据加密标准。之后，DES 成为金融界及其他非军事行业应用最为广泛的对称加密标准。DES 是分组密码的典型代表，也是第一个被公布出来的标准算法。DES 的算法完全公开，在密码学史上开创了先河。DES 是迄今为止世界上应用最为广泛的一种分组密码算法。DES 的研究大大丰富了设计和分析分组密码的理论、技术和方法。针对 DES，人们研制了各种各样的分析分组密码的方法，如差分分析方法和线性分析方法，这些方法对 DES 的安全性有一定的威胁，但没有真正对 16 轮 DES 安全性构成威胁。自从 DES 公布之日起，人们就认为 DES 的密钥长度太短（只有 56 比特），不能抵抗最基本的攻击方法——穷搜索攻击。

目前，国际上公开的分组密码算法有 100 多种，如，Lucifer、IDEA、SAFER，k-64、RC5、Skipjack、RC2、FEAL-N、REDOC-II、L0KI、CAST、Khuf u、Khafre、MMB、3-WAY、TEA、MacGuffin、SHARK、BEAR、LION、CA.1.1、CRAB、Biowfish、G0 ST、SQUARE 和 MISTY 等。

按密钥类型的不同，加密算法有对称密钥算法和非对称密钥算法。

### 1．对称加密算法

对称加密又称单钥密码或私钥密码，它采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用做解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难，除了数据加密标准（DNS），另一个对称密钥加密系统是国际数据加密算法（IDEA），它比 DNS 的加密性好，而且对计算机功能要求也没有那么高。IDEA 加密标准由 PGP（Pretty Good Privacy）系统使用。

根据密码算法对明文处理的方式标准不同，还可以将对称加密分为序列密码和分组密码两大类。

序列密码也称为流密码，其思想起源于 20 世纪 20 年代，最早的二进制序列密码系统是 Vernam 密码。Vernam 密码将明文消息转化为二进制数字序列，密钥序列也为二进制数字序列，加密是按明文序列和密钥序列逐位模 2 相加（即异或操作 XOR）进行，解密也是按密文序列和密钥序列逐位模 2 相加进行。

分组密码的加密方式是先将明文序列以固定长度进行分组，然后将每一组明文用相同的密码和加密函数进行运算，其中，在加密端当信息源发送数据之前，首先根据加密系统的要

求，将明文分成等长的分组（如分组 1、分组 2 等），然后每一个分组依次进入“加密器”与“加密密钥流”进行函数运行，实现加密操作。需要注意的是：每次进入“加密器”的分组不同，但对每一个分组进行加密的“加密密钥流”是相同的。在解密端的操作与加密端类似。

**2．非对称加密算法**

1976 年，美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全媒体上的通信双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，那么只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。非对称加密又称双钥密码或公钥加密。

## 8.3.2 认证技术

网络安全认证技术是网络安全技术的重要组成部分之一。认证指的是证实被认证对象是否属实和是否有效的一个过程。其基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、数字签名或者如指纹、声音、视网膜这样的生理特征。认证常常被用于通信双方相互确认身份，以保证通信的安全。认证技术一般可以分为两种：身份认证和消息认证。

**1．身份认证技术**

认证（Authentication）是证实实体身份的过程，是保证系统安全的重要措施之一。当服务器提供服务时，需要确认来访者的身份，访问者有时也需要确认服务提供者的身份。

身份认证是指计算机及网络系统确认操作者身份的过程。计算机网络系统是一个虚拟的数字世界，在这个数字世界中，一切信息包括用户的身份信息都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。而现实世界是一个真实的物理世界，每个人都拥有独一无二的物理身份。如何保证以数字身份进行操作的操作者就是这个数字身份的合法拥有者，也就是说，保证操作者的物理身份与数字身份相对应，就成为一个很重要的问题。身份认证技术的诞生就是为了解决这个问题。

现在计算机及网络系统中常用的身份认证方法包括基于口令的认证方法、双因素认证、一次口令机制、生物特征认证、USB Key 认证等。

**2．消息认证技术**

随着网络技术的发展，对网络传输过程中信息的保密性提出了更高地要求，这些要求主要包括：

（1）对敏感的文件进行加密，即使别人截取文件也无法得到其内容。

（2）保证数据的完整性，防止截获人在文件中加入其他信息。

（3）对数据和信息的来源进行验证，以确保发信人的身份。

消息认证实际上是对消息本身产生一个冗余信息——MAC（消息认证码），消息认证码是利用密钥对要认证的消息产生数据块加密生成新的数据块。它对于要保护的信息来说是唯一的，因此可以有效地保护消息的完整性，以及实现发送方消息的不可抵赖和不能伪造。

消息认证技术可以防止数据的伪造和被篡改，以及证实消息来源的有效性，已广泛应用于信息网络。随着密码技术与计算机计算能力的提高，消息认证码的实现方法也在不断的改进和更新之中，多种实现方式会为更安全的消息认证码提供保障。

## 8.4　防火墙技术

Internet 的迅速发展和普及应用，为人们检索和共享信息资源提供了方便，但随之而来的是对信息资源的污染和破坏变得更容易了。为了保护数据和资源的安全，人们制造了防火墙。就像建筑防火墙或护城河能够保护建筑物及其内部资源安全或保护城市免受侵害一样，网络防火墙能够防止外部网络上的各种危害入侵到内部网络。

### 8.4.1　防火墙的功能

防火墙是计算机网络安全管理中应用最早和技术发展最快的安全产品之一。防火墙在加入网络后将形成一个安全节点，该节点同时具有阻塞和控制功能：用于阻塞进入该节点的未被允许的流量，通过控制功能决定哪些信息可以通过该节点，而哪些信息拒绝通过该节点。防火墙能够极大地提高被保护网络的安全性，并通过过滤不安全的服务而降低风险。

网络防火墙是企业内部网和外部网（Internet）之间所设立的执行访问控制策略的安全系统，它在内部网和 Internet 之间设置控制，以阻止外界对内部资源的非法访问，也可以防止内部对外部的不安全访问。设置防火墙的思想就是在内部、外部两个网络之间建立一个具有安全控制机制的安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对内部网服务和访问的安全审计和控制。

防火墙是一种由计算机硬件和软件组成的系统，它已成为实现网络安全策略的最有效地工具之一，并被广泛地应用到内部网上。通常情况下，内部网和 Internet 进行互联时，必须使用一个中间设备，这个设备既可以是专门的互联设备（如路由器或网关），也可以是网络中的某个节点（如一台主机）。这个设备至少具有两条物理链路，一条通往外部网络，一条通往内部网络。企业用户希望和其他用户通信时，信息必须经过该设备；同样，其他用户希望访问企业网时，也必须经过该设备。显然，该设备是阻挡攻击者入侵的关口，也是防火墙实施的理想位置，如图 8-6 所示防火墙的位置。

因此，可以说防火墙能够限制非法用户从一个被严格保护的设备上进入或离开，从而有效地阻止针对内部网的非法入侵。但由于防火墙只能对跨越边界的信息进行检测、控制，而对网络内部人员的攻击不具备防范能力，因此单独依靠防火墙来保护网络的安全性是不够的，还必须与入侵检测系统（IDS）、安全扫描等其他安全措施综合使用才能达到目的。

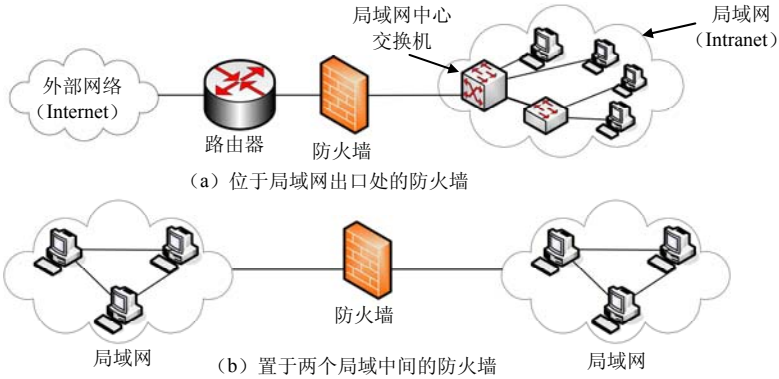



图 8-6　防火墙的位置

一般情况下，防火墙具有以下功能：

- 监控并限制访问；
- 控制协议和服务；
- 保护内部网络；
- 网络地址转换（NAT）；
- 虚拟专用网（VPN）；
- 日志记录与审计。

但防火墙也有不足之处，主要表现在以下几个方面。

- 防火墙不能防范未通过自身的网络连接；
- 防火墙不能防范全部的威胁；
- 防火墙不能防止感染了病毒的软件或文件的传输；
- 防火墙不能防范内部用户的恶意破坏；
- 防火墙本身也存在安全问题；
- 人为因素在很大程度上影响了防火墙的功能。

## 8.4.2　防火墙技术及分类

防火墙技术大体上可分为两类：网络层防火墙技术和应用层防火墙技术。这两个层次的防火墙分别被称作包过滤防火墙和代理服务器防火墙。

### 1．包过滤防火墙

网络层防火墙技术根据网络层的特点对传输的信息进行过滤。网络层技术的一个范例就是包过滤技术。因此，在网络层实现的防火墙也叫包过滤防火墙。

包过滤防火墙是在网络的出口（如路由器）对通过的数据包进行选择，只有满足条件的数据包才允许通过，否则被抛弃。这样可以有效地防止恶意用户利用不安全的服务对内部网进行攻击。

在网络上传输的每个数据包都可分为两个部分：数据部分和包头部分。包过滤器就是根据包头信息来判断该包是否符合网络管理员设定的规则表中的相应规则，以确定是否允许数据包通过。包过滤规则一般是基于某些或全部包头信息的，如 IP 协议类型、源地址、IP 选择、

域的内容、TCP 源端口号、TCP 目标端口号等。例如，包过滤防火墙可以对来自特定的 Internet 地址的信息进行过滤，或者只允许来自特定地址的信息通过。它还可以根据需要的 TCP 端口来过滤信息。如果将过滤器设置成只允许数据包通过 TCP 端口 80（标准的 HTTP 端口），那么在其他端口，如端口 25（标准的 SMTP 端口）上的任何数据包均不得通过。

包过滤防火墙既可以允许授权的服务程序和主机直接访问内部网络，也可以过滤指定的端口和内部用户的 Internet 地址信息，限制内部网络对外部网络的访问。大多数包过滤防火墙的功能可以设置在内部网络与外部网络之间的路由器上。

**2．代理服务器防火墙**

应用层防火墙技术控制对应用程序的访问。应用层防火墙也称为代理服务器，它能够代替网络用户完成特定的 TCP/IP 功能。一个代理服务器本质上是一个应用层网关，即一个为特定网络应用而连接两个网络的网关。用户就某一项 TCP/IP 应用（如 HTTP），同代理服务器打交道，代理服务器要求用户提供其要访问的外部 Internet 主机名。当用户答复并提供了正确的用户身份及认证信息后，代理服务器建立与外部 Internet 主机的连接，为两个通信点充当中继。代理服务器防火墙分别与内部和外部系统连接，不允许信息越过防火墙而传输，整个过程可以对用户完全透明。用户提供的用户身份及认证信息可用于用户级的认证。最简单的情况是它只由用户标识和口令构成。但是如果防火墙是通过 Internet 可访问的，则应该使用更强的认证机制。

代理服务器防火墙还能记录通过它的一些信息，如什么用户在什么时间访问过什么站点。这些审计信息可以帮助网络管理员识别网络间谍。有些代理服务器还可存储 Internet 上那些被频繁访问的页面，这样当用户请求访问这些页面时，服务器本身就能提供这些页面而不必连接到 Internet 上的服务器，从而缩短了访问这些页面的内部响应时间。许多代理服务器防火墙除了提供代理请求服务外，还提供网络层信息过滤的功能。

包过滤防火墙与代理服务器防火墙相比，具有价格便宜、安装和管理简单等优点，但其功能单一，应用的灵活性和安全性较差。包过滤防火墙一般用在互连结构简单、拥有的系统没有很大风险、安全性要求不高的场合；而代理服务器防火墙可用于系统复杂、安全性和可靠性要求高、功能要求齐全、拥有大量网络安全资金、拥有管理代理服务器防火墙的软件和硬件技术的场合。

但是随着以家庭用户为代表的个人计算机的不断普及，个人防火墙技术开始出现并得到了广泛的应用。个人防火墙是一套安装在个人计算机上的软件系统，它能够监视计算机的通信状况，一旦发现有对计算机产生危险的通信就会报警通知管理员或立即中断网络连接，以此实现对个人计算机上重要数据的安全保护。个人防火墙的主要功能是：防止 Internet 用户的攻击；阻断木马及其他恶意软件的攻击；为移动计算机提供安全保护；与其他安全产品进行集成。个防火墙的主要技术是：基于应用层网关；基于 IP 地址和 TCP/UDP 端口的安全规则；端口“隐蔽”功能；邮件过滤功能。

## 8.4.3　防火墙应用系统

一般，构成防火墙的体系结构有 3 种：双穴主机结构、主机过滤结构和子网过滤结构。

如下是按照这 3 种体系结构构建的防火墙应用系统介绍。

### 1．双穴主机结构防火墙

双穴（Dual Homed）主机结构防火墙是围绕着具有双穴结构的主计算机而构建的，如图 8-7 中的线框内部分所示。双穴主机具有两个或两个以上接口，这种结构的主机可担任与这些接口连接的网络路由器。双穴主机分别与受保护的内部子网及 Internet 连接，起着监视和隔离应用层信息流的作用，彻底隔离了所有的内部主机与外部主机的直接连接。

双穴主机可与内部网系统通信，也可与外部网系统通信。借助于双穴主机，防火墙内外两网的计算机便可（间接）通信了。即内外网的主机不能直接交换信息，信息交换要由该双穴主机“代理”并“服务”，因此该主机也相当于代理服务器。因而，内部子网十分安全。内部主机通过双穴主机防火墙（代理服务器）得到 Internet 服务，并由该主机集中进行安全检查和日志记录。双穴主机防火墙工作在 OSI 的最高层，它掌握着应用系统中可用做安全决策的全部信息。

### 2．主机过滤结构防火墙

双穴主机防火墙是由一台同时连接内外部网络的双穴主机提供安全保障的，而主机过滤防火墙则与之不同。它是由一台过滤路由器与外部网络相连，再通过一个可提供安全保护的主机（堡垒主机）与内部网络连接。来自外部网络的数据包先经过包过滤路由器过滤，不符合过滤规则的数据包被过滤掉；符合规则的数据包则被传送到堡垒主机上。堡垒主机上的代理服务器软件将允许通过的信息传输到受保护的内部网络上，如图 8-8 所示。主机过滤防火墙结构中堡垒主机是 Internet 主机连接内部网系统的桥梁。任何外部系统要访问内部网系统或服务，都必须连接到该主机上。因此该主机需要高级别安全。

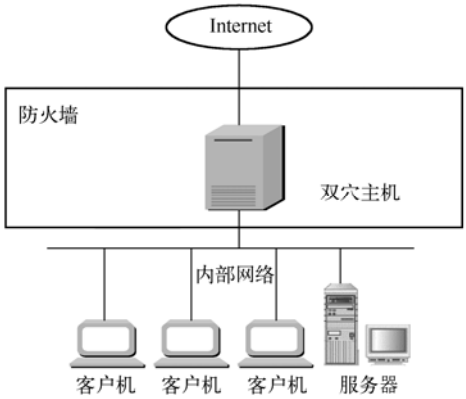



图 8-7　双穴主机结构防火墙

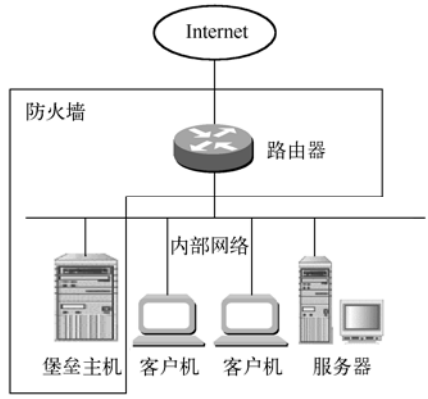



图 8-8　主机过滤结构防火墙

### 3．子网过滤结构防火墙

子网过滤结构是在主机过滤体系结构中又增加了一个额外的安全层次。增加的安全层次包括一台堡垒主机和一台路由器。两路由器之间是一个被称为周边网络或参数网络的安全子网，也叫“非军事区网 DMZ”。这就使得内部网和外部网之间有了两层隔断。这种结构就是使用两个过滤路由器和一个堡垒主机形成了一个复杂的防火墙，以进行安全控制。

堡垒主机通过内部、外部两个路由器与内部、外部网络隔开，这样可减小堡垒主机被侵

袭的影响。被保护的内部子网主机置于内部包过滤路由器内，堡垒主机被置于内部和外部包过滤路由器之间。子网过滤体系结构的最简单的形式为两个过滤路由器，每一个都连接到参数网络上，一个位于参数网与内部网之间；另一个位于参数网与外部网之间，如图 8-9 所示。这是一种比较复杂的结构，它提供了比较完善的网络安全保障和较灵活的应用方式。

周边网络是在内部和外部两网络之间另加的一层安全保护层，相当于一个应用网关，堡垒主机上运行应用代理服务器软件。同时，企业的对外信息服务器（如 WWW、FTP 服务器等）也可设置在 DMZ 内。

如果入侵者成功地闯过外层保护网到达防火墙，周边网络就能在入侵者与内部网之间再提供一层保护。如果入侵者仅仅侵入到周边网络的堡垒主机，他只能偷看到周边网络的信息流而看不到内部网的信息。周边网络的信息流仅往来于外部网到堡垒主机，没有内部网主机间的信息流在周边网络中流动，所以堡垒主机受到损害也不会破坏内部网的信息流。

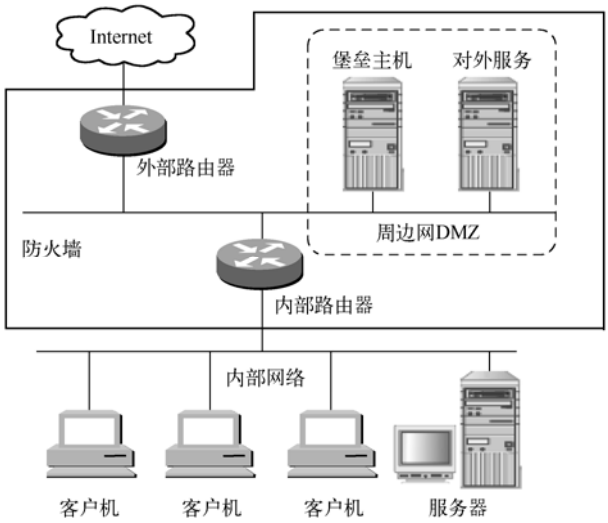



图 8-9　子网过滤结构防火墙

在内、外部两个路由器上建立包过滤都设置了包过滤规则，两者的包过滤规则基本上相同。内部路由器完成防火墙的大部分包过滤工作，它允许某些站点的包过滤系统认为符合安全规则的服务在内/外部网之间互传。内部路由器的主要功能就是保护内部网免受来自外部网与周边网络的侵扰，外部路由器既保护周边网络又保护内部网络。实际上，在外部路由器上仅做一小部分包过滤，它几乎让所有周边网络的外向请求通过。外部路由器的包过滤主要是对周边网络上的主机提供保护。

# 练习 8

## 一、填空题

（1）网络系统的安全性的含义可包括系统的_____性、软件和数据的_____性、可用性和保密性等几个特征。

（2）_____威胁是在无预谋的情况下破坏了系统的安全性、可靠性或资源的完整性等；_____威胁实际上就是“人为攻击”。

（3）_____攻击是指攻击者只通过观察网络线路上的信息，而不干扰信息的正常流动；_____攻击是指攻击者对传输中的信息或存储的信息进行各种非法处理，有选择地更改、插入、延迟、删除或复制这些信息。

（4）计算机病毒是一种能破坏计算机系统资源的特殊_____。

（5）计算机病毒具有_____性、_____性、潜伏性、触发性和破坏性。

（6）加密算法除了提供信息的_____性之外，它和其他技术结合，还能提供信息的_____性。

（7）按密钥类型的不同，加密算法有_____算法和_____算法。

（8）网络安全认证技术一般可以分为两种：_____认证和_____认证。

（9）网络防火墙是在_____之间所设立的执行_____策略的安全系统。

（10）应用层防火墙也称为_____服务器，它能够代替网络用户完成特定的 TCP/IP 功能。

（11）在 OSI 管理标准中，将系统管理功能分为_____管理、_____管理、性能管理、安全管理和计费管理。

（12）SNMP 模型组成的 4 个要素是：_____、_____、管理信息库（MIB）和网络管理协议（SNMP）。

## 二、选择题

（1）包过滤防火墙属于（　　）防火墙技术。

A．网络层　　B．传输层　　C．应用层　　D．其他层

（2）Windows NT 可达到的安全级别为（　　）。

A．A1 级　　B．B2 级　　C．C2 级　　D．D1 级

（3）连通性测试程序是（　　）。

A．ping　　B．Netstat　　C．Tracert　　D．Ipconfig

（4）利用（　　）工具可以查看和修改网络中的 TCP/IP 协议的有关配置信息。

A．ping　　B．Netstat　　C．Tracert　　D．Ipconfig

（5）当管理代理发现被管对象出现严重错误时，立即使用（　　）命令向网络管理站报警，且不须等待接收方响应。

A．get　　B．get next　　C．set　　D．trap

## 三、简答题

（1）如何理解网络安全?

（2）试描述防火墙的基本功能。

（3）网络管理的基本功能有哪些?各功能所涉及的主要内容是什么?

（4）试述 SNMP 模型的组成及各组成部分的作用。

# 第 9 章

# 基础实验与综合实训指导

## 实验 1　传输介质认识与网线制作

**【实际应用背景描述】**

你是公司的网络管理员，随着公司规模的扩大，公司购置了新的计算机，并且需要将新添置的计算机连接在公司局域网中，使其能够与其他计算机正常通信。首先你需要做一根合格的双绞线将计算机和公司的局域网进行物理连接。

### 一、实验目的

（1）了解 LAN 中常用的几种传输介质、连接器的性能及各自特点。
（2）理解直通线和交叉线的应用范围，掌握双绞线中的直通线和交叉线的制作方法。
（3）掌握网线制作工具、电缆测试仪的使用方法。

### 二、实验任务与要求

（1）掌握 LAN 中常用的几种传输介质、连接器的连接方法和实际使用。
（2）独立制作一根合格的直通双绞线和一根交叉双绞线。
（3）完成一定数量的网络跳线的压接操作。

### 三、实验设备

实验所需设备有五类双绞线、RJ-45 水晶头、压线钳、电缆测试仪、剥线钳、打线刀、剪刀、端接及压接线实验装置等。

### 四、实验相关知识

目前计算机局域网络的有线通信常用的传输介质有同轴粗缆与细缆，无屏蔽双绞线（UTP）、光纤等。不同的传输介质具有不同的电气特性、机械特性和信息传输格式，因此它

们也就具有不同的传输方式、传输速率、传输距离等。在组建局域网时，要根据具体情况（如覆盖范围、应用对象、性能要求、资金情况等）来决定采用何种网络拓扑结构、传输介质及相关的网络连接设备等。

（1）双绞线：双绞线是由两根绝缘金属线互相缠绕而成的，这样的一对线作为一条通信链路，由 4 对双绞线构成双绞线电缆。双绞线点到点的通信距离一般不超过 100m。目前，计算机网络上用的双绞线有 3 类（最高传输速率为 10Mbps）、五类线（最高传输速率为 100Mbps）、超五类线和六类线（传输速率至少为 250Mbps）、七类线（传输速率至少为 600Mbps）。双绞线电缆的连接器一般为 RJ-45。

（2）同轴电缆：同轴电缆由内、外两个导体组成，内导体可以由单股或多股线组成，外导体一般由金属丝编织网组成。内、外导体之间有绝缘材料，其匹配阻抗为 50Ω。同轴电缆分为粗缆和细缆，粗缆用 DB-15 连接器，细缆用 BNC 和 T 形连接器。

（3）光缆：光缆由两层折射率不同的材料组成。内层是具有高折射率的玻璃单根纤维体组成，外层包一层折射率较低的材料。光缆的传输形式分为单模传输和多模传输，单模传输性能优于多模传输，所以光缆从工程应用角度分为单模光缆和多模光缆，单模光缆传输距离为几十公里，多模光缆为几公里，光缆的传输速率可达到每秒几百兆位，光缆用 ST 或 SC 连接器。

（4）线序标准：1995 年年底，EIA/TIA 568 标准正式更新为 EIA/TIA568A，EIA/TIA 的布线标准中规定了两种双绞线的线序 T568A 与 T568B。

标准　T568A：1—绿白，2—绿，3—橙白，4—蓝，5—蓝白，6—橙，7—棕白，8—棕；

标准　T568B：1—橙白，2—橙，3—绿白，4—蓝，5—蓝白，6—绿，7—棕白，8—棕；

（5）双绞线种类：一根接好插头的双绞线一般有 3 种，不同双绞线的用途如表 9-1 所示。

表 9-1　不同双绞线的用途

| 网线的用途 | 水晶头的做法 |
| --- | --- |
| 交换机/集线器（Hub）↙↙计算机 | B↙↙B |
| 计算机 ↙↙ 计算机的连接 | B↙↙A |
| 交换机/Hub ↙↙下级交换机/Hub（普通口） | B↙↙A |
| 交换机/Hub↙↙下级交换机/Hub（uplink 口） | B↙↙B |

直通（Straight-through）线：一般用来连接两个不同性质的接口。一般用于：PC to Switch/Hub，Router to Switch/Hub。直通线的做法就是使两端的线序相同，要么两头都是 T568A 标准，要么两头都是 T568B 标准。

交叉（Cross-over）线：一般用来连接两个性质相同的端口。比如，Switch to Switch，Switch to Hub，Hub to Hub，Host to Host，Host to Router。做法就是使两端的线序不同，一头做成 T568A，一头做成 T568B 即可。

全反（Rolled）线：不用于以太网的连接，主要用于主机的串口和路由器（或交换机）console 口的连接。做法就是使线的一端的顺序是 1～8，另一端则是 8～1 的顺序。

## 五、实验内容及步骤

（1）传输介质认识：对照以前所学习的知识，分别仔细查看双绞线及光纤的结构特点；

弄清 RJ-45 头、BNC 接头、T 形头等各种连接器所对应的网线类型、连线方式、压接方法，每种网线（带连接器）连接的相关设备及应用场合。

（2）双绞网线制作与测试、所需工具、双绞线压线钳及电缆测试仪。

① 所需工具：双绞线压线钳（如图 9-1 所示）及便携式电缆测试仪（如图 9-2 所示）。

其中，便携式网线测试仪通过自动扫描电缆专用于快速测试电缆的连接性线序及定位，通过附带的远程终结器（该测试器）无论在电缆安装前后，都能测试电缆，非常方便。

② 制作步骤：

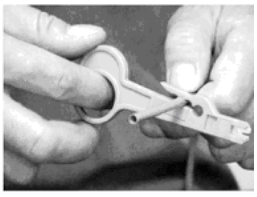
**【步骤 1】**利用斜口钳剪下所需要的双绞线长度，然后再利用双绞线剥线器（实际用什么剪都可以）将双绞线的外皮除去 2～3cm。剥线完成后的双绞线电缆如图 9-3 所示。

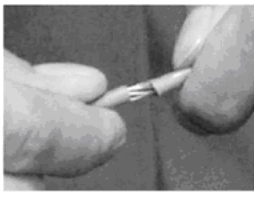
RJ-45 工具

图 9-1　双绞线压线钳

图 9-2　便携式电缆测试仪

剥 PVC 线缆护套





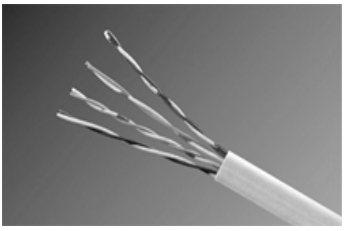


图 9-3　剥去外护套

**【步骤 2】**接下来就要进行拨线的操作。将裸露的双绞线中的橙色对线拨向自己的前方，棕色对线拨向自己的方向，绿色对线剥向左方，蓝色对线剥向右方，如图 9-4 所示（上：橙、左：绿、下：棕、右：蓝）。

**【步骤 3】**将绿色对线与蓝色对线放在中间位置，而橙色对线与棕色对线保持不动，即放在靠外的位置，如图 9-5 所示（左一：橙、左二：绿、左三：蓝、左四：棕）。小心地剥开每一对线，因为遵循 EIA/TIA568B 的标准来制作接头，所以线对颜色是有一定顺序的（如图 9-6 所示）。

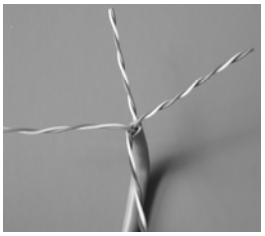


图 9-4　拨线图

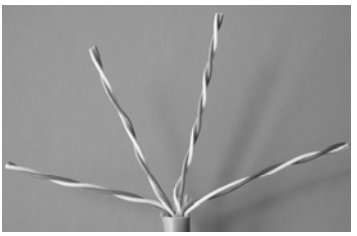


图 9-5　调整线对的位置

需要特别注意的是，T568B 线序标准中绿色条线应该跨越蓝色对线。这里最容易犯错的

地方就是将白绿线与绿线相邻放在一起，这样会造成串扰，使传输效率降低。

**【步骤 4】**将裸露出的双绞线捋直并按 T568B 线序标准排好，用剪刀或斜口钳剪下只剩约 14mm 的长度，之所以留下这个长度是为了符合 EIA/TIA 的标准，如图 9-7 所示。

**【步骤 5】**最后再将双绞线的每一根修剪后的线依序插入 RJ-45 水晶头内，注意线对应全部顶到头，外护套应进入水晶头内，第一只引脚内应该放白橙色的线，其余类推，如图 9-8 所示。

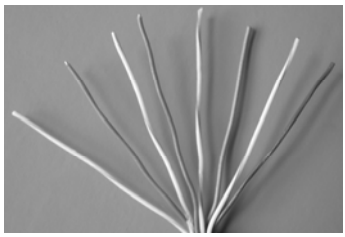


图 9-6　剥开每一对绞线

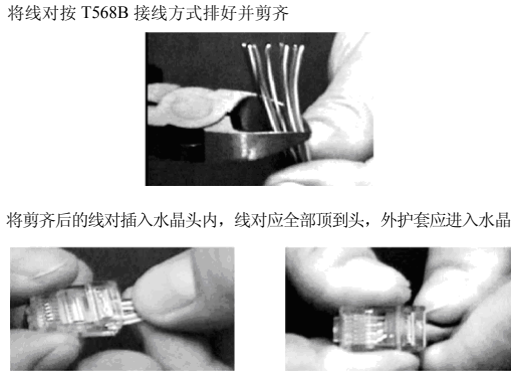



图 9-7　剪掉多余的导线


图 9-8　将修剪后的双绞线插入 RJ-45 水晶头

**【步骤 6】**确定双绞线的每根线已经正确放置之后，就可以用 RJ-45 压线钳压接 RJ-45 接头，市面上还有一种 RJ-45 接头的保护套，可以防止接头在拉扯时造成接触不良。使用这种保护套时，需要在压接 RJ-45 接头之前就将这种胶套插在双绞线电缆上。完成的 RJ-45 接头应该如图 9-9 所示。

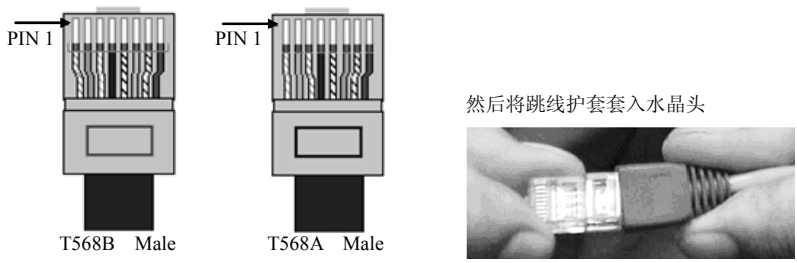



图 9-9　完成连接的 RJ-45 接头

为了保持最佳的兼容性，普遍采用 EIA/TIA568B 标准来制作网线。注意：在整个网络布线中应该只采用一种网线标准。如果标准不统一，几个人共同工作时准会乱套；更严重的是施工过程中一旦出现线缆差错，在成捆的线缆中是很难查找和剔除的。强烈建议统一采用 T568B 标准。

**【步骤 7】**测试：两端制作连接好 RJ-45 插头后，使用便携式线缆测试仪进行测试。如果压接正确时，对应的指示灯亮显示；如果压接不正确或者没有实现电气连接时，对应的指示灯不亮。

## 六、思考题

（1）A 线序和 B 线序有何区别？若不遵循上述标准，是否所做的网线不可用？

（2）对于主机来说，交换机和路由器都属于异种设备，为什么交换机用直连线，而路由器用交叉线？

（3）现在只有直连线若干，同时还有一个交换机和一个路由器，如果需要建立主机和路由器之间的连接可以采取什么方式实现？

# 实验 2　TCP/IP 配置及主机互连

**【实际应用背景描述】**

你是公司的网络管理员，当公司网络出现异常时，能够使用所掌握的网络命令对网络故障进行检查和排除。

## 一、实验目的

（1）熟悉掌握主机互连常用设备的基本使用方法。

（2）测试验证实验环境网络拓扑，掌握 TCP/IP 基本配置。

（3）熟悉了解双网卡的配置及使用方法。

## 二、实验设备（为每一实验小组提供如下实验设备）

（1）实验台设备：计算机两台 PC1 和 PC2。

（2）实验机柜设备：

- S3550（S3760）三层交换机一台；
- S2126 二层交换机一台。

（3）实验工具及附件：网线测试仪一台，跳线若干。

## 三、实验内容及要求

（1）熟悉实验室环境，了解实验设备及相关管理设备的基本布置。
（2）熟练掌握常用组网设备的基本使用方法和基本配置方法，实现主机互连。
（3）测试验证网络连通性，画出本实验小组的网络拓扑图。
（4）练习常用网络测试工具软件的使用。

## 四、实验步骤

（1）画出所属实验小组的实验设备的布置示意图，并标明实验设备编号（型号、组号、标号等）。

（2）通过观察，测试验证所属实验小组的物理拓扑（本小组的所有计算机与网络设备的物理连接形式），画出物理拓扑图。

（3）分别使用命令行和图形界面方式查看实验所用计算机上安装网卡的数量、产品型号以及在操作系统里设置的名称、主机的 TCP/IP 基本配置信息，并记录显示结果。

**【步骤 1】**使用命令行方式，如图 9-10 所示打开 cmd 命令行窗口，启动后界面如图 9-11 所示。

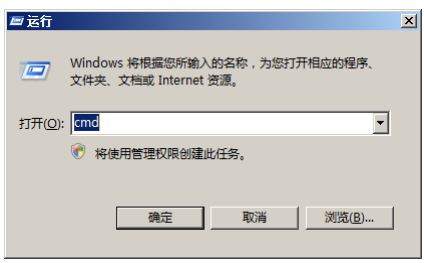



图 9-10　启动命令窗口图

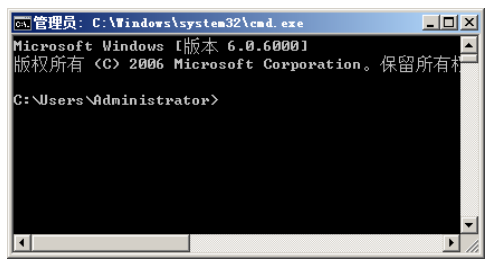



图 9-11　DOS 命令提示符界面

**【步骤 2】**在命令提示符下输入 ipconfig/all 命令，查看命令运行结果。如图 9-12 所示，通过观察输出信息的内容，确定当前计算机的如下 TCP/IP 配置信息。

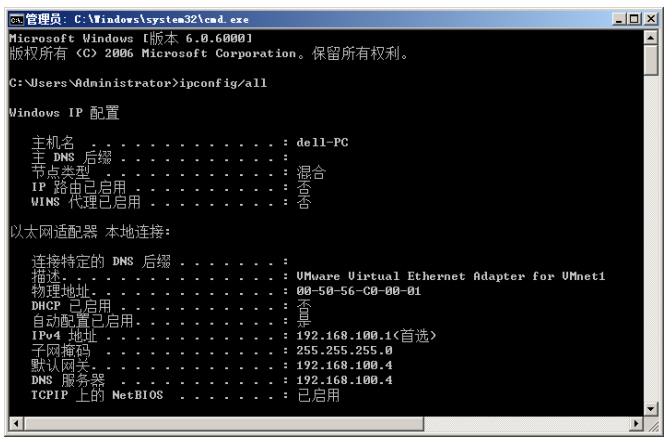



图 9-12　用 ipconfig/all 命令检查计算机 TPC/IP 设置

- 计算机安装的网卡的数量；
- 每块网卡的型号；
- 每块网卡在操作系统内显示的名称；
- 每块网卡当前绑定的 IP 地址；
- 网卡的物理地址（MAC 地址）；
- 默认网关的 IP 地址及 DNS 服务器的 IP 地址。

**【步骤 3】**利用图形界面设置主机 IP 地址及修改计算机名称。

将网络中计算机的 IP 址依次设为：192.168.0.1、192.168.0.2、192.168.0.3、192.168.0.4 等（以此类推）。设置步骤如下：

- 在“网上邻居”图标上右击，选择“属性”选项，再右击“本地连接”图标，选择“属性”选项，打开“本地连接属性”对话框，如图 9-13 所示。
- 双击“Internet 协议（TCP/IP）属性”，打开如图 9-14 所示对话框。


图 9-13 “本地连接属性”对话框

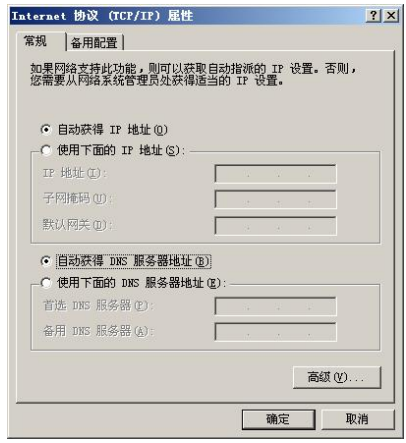



图 9-14 “Internet 协议（TCP/IP）属性”对话框

- 选中“使用下面的 IP 地址”单选按钮，改变 IP 地址设置方式为静态方式，如图 9-15 所示。
- 输入 IP 地址、子网掩码、默认网关、DNS 服务器等内容，如图 9-16 所示。

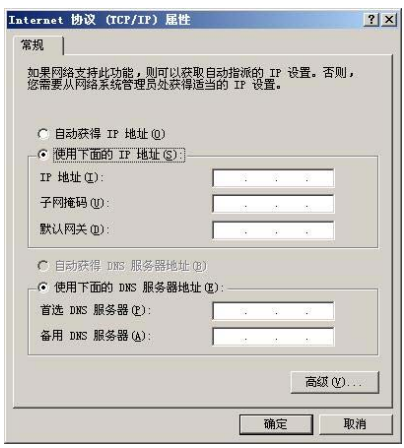



图 9-15　选择 IP 地址配置方式

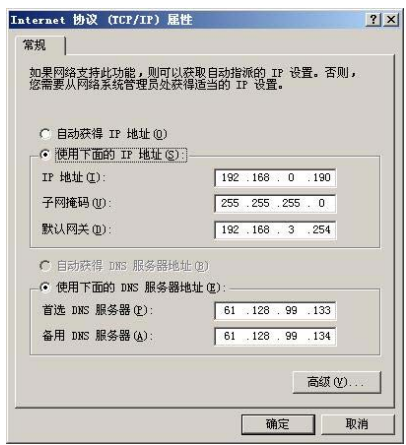



图 9-16　手工方式设置静态

- 为计算机指定计算机名，在桌面“我的电脑”图标上右击，选择“属性”命令，在打开的对话框中切换到“计算机名”选项卡，如图 9-17 所示。
- 单击“更改”按钮，输入计算机名和所在工作组名，如图 9-18 所示。

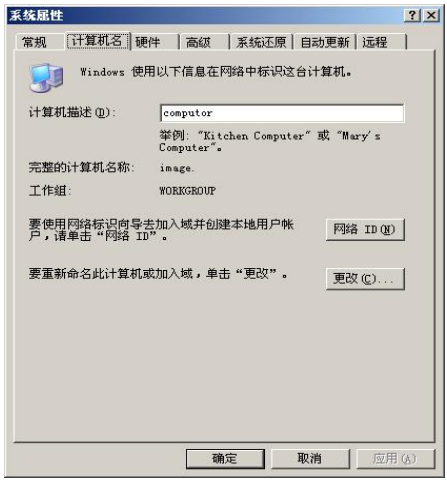



图 9-17 “系统属性”对话框


图 9-18 修改计算机名称

- 重新启动计算机，以使上面的修改设置生效。

（4）组建对等式局域网（即利用交换机实现主机互联互通）并测试网络连通性：

实验原理图如图 9-19 所示。

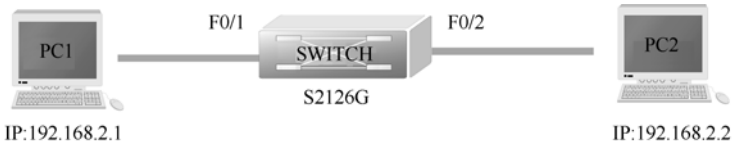



图 9-19 主机互连原理示意图

**注意**：在有些实验环境下，交换机的端口是通过双绞线跳接至配线架的，在这种情况下，接线只能在配线架上进行，如果没有使用配线架则可以直接用双绞线将计算机连接在交换机的以太网端口上。

实验具体步骤：

（1）设置计算机 PC1 的 IP 地址及子网掩码分别为：192.168.2.1 和 255.255.255.0。

（2）设置计算机 PC2 的 IP 地址及子网掩码为：192.168.2.2 和 255.255.255.0。

（3）将两台计算机的网卡分别与交换机的 F0/1 和 F0/2 口连接。

（4）使用 ping 命令测试网络连通性（测试方法参照下面实验内容 5 中 ping 命令的介绍）。

（5）TCP/IP 的常用测试工具：

① ipconfig——显示 IP 配置信息。

```
c:\>ipconfig/?              显示帮助信息
c:\>ipconfig /all           显示 IP 配置的详细信息
```

② ping——测试网络连通性。

应用举例：c:\>ping 192.168.1.101　　测试与 IP 地址为 192.168.1.101 的主机的连通性

- c:\>ping 192.168.1.101 –t　　连续测试
- c:\>ping 192.168.1.101 –n 10　　发送 10 个测试数据包
- c:\>ping 192.168.1.101 –l 1024　发送数据包的长度为 1 024 字节

③ route——显示和修改本地路由表。

- c:\>route print　　显示路由表：
- c:\>route ADD 157.0.0.0 MASK 255.0.0.0 192.168.100.3　　添加路由表项
- c:\>route delete 157.0.0.0　　删除路由表项：

④ arp——显示或设置 IP 地址与 MAC 地址的对应关系。

- c:\>arp –g　　查看 ARP 缓存
- c:\>arp –a
- c:\>arp -s 157.55.85.212 00-aa-00-62-c6-09　　添加静态 ARP 映射
- c:\>arp –d 157.55.85.212　　删除 ARP 映射

⑤ tracert——跟踪数据包到达目的地所采取的路由。

- c:\>tracert 192.168.1.101

⑥ pathping——跟踪路由和测试连通性。

- c:\>pathping 192.168.1.2

⑦ hostname——返回本地计算机的主机名。

- c:\>hostname

⑧ netstat——显示当前 TCP/IP 网络连接，并统计会话信息。

- c:\>netstat /?　　显示帮助信息
- c:\>netstat –na　　显示所有已建立的有效连接与信息列表

⑨ nbtstat——显示本地 NETBIOS 名称列表与 NETBIOS 名称缓存。

- c:\>nbtstat /?　　显示帮助信息
- c:\>nbtstat –n　　查看注册的 NETBIOS 名称

## 五、思考题

（1）要使用 TCP/IP 协议，计算机必须设置的是什么？
（2）在 Windows 网络中，除使用 TCP/IP 协议外，还可以使用哪些协议？
（3）一块网卡能不能设置多个 IP 地址？

# 实验 3　IP 地址规划

**【实际应用背景描述】**

你是某公司的 IT 技术部员工，公司通过 Internet 服务提供商（Internet Service Provider，ISP）得到一个地址段 200.13.14.0，并将企业办公室计算机接入 Internet。公司要求你所在的部门对整个公司的 IP 地址进行规划和设计。

## 一、实验目的

（1）掌握子网规划的方法。
（2）掌握在内部局域网上划分逻辑子网、应用和测试的方法。
（3）理解 IP 协议与 MAC 地址的关系。

## 二、实验任务与要求

（1）在内部局域网上划分逻辑子网。
（2）对划分的逻辑子网进行应用和测试。

## 三、实验设备

（1）实验台设备：计算机两台 PC1 和 PC2。
（2）实验机柜设备：S2126 二层交换机一台。
（3）实验工具及附件：网线测试仪一台，跳线若干。

## 四、实验相关知识

### 1．子网编址的方法

IP 地址具有层次结构，标准的 IP 地址分为网络号和主机号两层。为了避免 IP 地址的浪费，子网编址的主机号部分进一步划分成子网部分和主机部分，如图 9-20 所示。


图 9-20　子网编址的层次结构

为了创建一个子网地址，网络管理员从标准 IP 地址的主机号部分“借”位并把它们指定

为子网号部分。只要主机号部分能够剩余两位，子网地址可以借用主机号部分的任何位数（但至少应借用两位），因为 B 类网络的主机号部分只有两个字节，因此最多只能借用 14 位创建子网。而在 C 类网络中，由于主机号部分只有一个字节，故最多只能借用 6 位去创建子网。

### 2．子网的规划方法

子网规划，就是根据子网个数要求及每一个子网的有效主机地址个数要求，确定借几位主机号作为子网号，然后写出借位后的子网个数、每一个子网的有效主机地址个数、每一个子网的子网地址、子网掩码和每一个子网的有效主机地址。子网规划和 IP 地址分配在网络规划中占有重要地位。在确定借几位主机号作为子网号时应使子网号部分产生足够的子网，而剩余的主机号部分能容纳足够的主机。

与标准的 IP 地址相同，子网编址也为子网网络和子网广播保留了地址编号。在子网编址中以二进制数全“0”结尾的 IP 地址是子网地址，用来表示子网；而以二进制数全“1”结尾的 IP 地址则是子网直接广播地址，为子网广播所保留。由于这个 C 类地址最后一个字节的 4 位用做划分子网，因此子网中的主机号只能用剩下的 4 位来表达。在这 4 位中，全部为“0”的表示该子网网络，全部为“1”的表示子网广播，其余的可以分配给子网中的主机。

IP 协议规定，将与 IP 地址的网络号和子网号部分相对应的位用“1”、与 IP 地址的主机号部分相对应的位用“0”表示后，就得出了该 IP 地址对应的子网掩码。将 IP 地址和它的子网掩码相结合，就可以判断出 IP 地址中哪些位表示网络和子网，哪些位表示主机。

### 3．在内部局域网上划分逻辑子网

尽管子网编址的初衷是为了避免小型或微型网络浪费 IP 地址，但是，有时候将一个大规模的物理网络划分成几个小规模的子网还有其他的好处：由于各个子网在逻辑上是独立的，因此没有路由器的转发，尽管这些主机处于同一个物理网络中，但子网之间的主机不可能相互通信。

## 五、实验步骤

在子网划分方案定好之后，就可以动手修改计算机的配置了，配置方法参照实验二。

实验原理图如图 9-21 所示。


图 9-21　主机互连原理示意图

**注意**：在有些实验环境下，交换机的端口是通过双绞线跳接至配线架的，在这种情况下，接线只能在配线架上进行，如果没有使用配线架则可以直接用双绞线将计算机连接在交换机的以太网端口上。

**【步骤 1】**

（1）两人一组，根据实验原理图 9-22，设置两台主机的 IP 地址与子网掩码：

PC1: 10.2.2.2　　255.255.254.0

PC2: 10.2.3.3　　255.255.254.0

（2）两台主机均不设置默认网关。

（3）用 arp -d 命令清除两台主机上的 ARP 表，然后在 PC1 与 PC2 上分别用 ping 命令与对方通信，观察并记录结果，并分析原因。

（4）在两台 PC 上分别执行 arp -a 命令，观察记录结果，并分析原因。

**提示**：由于主机将各自通信目标的 IP 地址与自己的子网掩码相“与”后，发现目标主机与自己均位于同一网段（10.2.2.0），因此通过 ARP 协议获得对方的 MAC 地址，从而实现在同一网段内网络设备间的双向通信。

**【步骤 2】**

（1）将 PC1 的子网掩码改为：255.255.255.0，其他设置保持不变。

（2）在两台 PC 上分别执行 arp-d 命令清除两台主机上的 ARP 表。然后在 A 上“ping” PC2，观察并记录结果。

（3）在两台 PC 上分别执行 arp -a 命令，观察记录结果，并分析原因。

**提示**：PC1 将目标设备的 IP 地址（10.2.3.3）和自己的子网掩码（255.255.255.0）相“与”得 10.2.3.0，和自己不在同一网段（PC1 所在网段为：10.2.2.0），则 PC1 必须将该 IP 分组首先发向默认网关。

**【步骤 3】**

（1）按照实验 2 的配置，接着在 PC2 上“ping”PC1，观察记录结果，并分析原因。

（2）在 PC2 上执行 arp -a 命令，观察记录结果，并分析原因。

**提示**：PC2 将目标设备的 IP 地址（10.2.2.2）和自己的子网掩码（255.255.254.0）相“与”，发现目标主机与自己均位于同一网段（10.2.2.0），因此，PC2 通过 ARP 协议获得 PC1 的 MAC 地址，并可以正确地向 PC1 发送 Echo Request 报文。但由于 PC1 不能向 PC2 正确地发回 Echo Reply 报文，故 PC2 上显示 ping 的结果为“请求超时”。

在该实验操作中，通过观察 PC1 与 PC2 的 ARP 表的变化，可以验证：在一次 ARP 的请求与响应过程中，通信双方就可以获知对方的 MAC 地址与 IP 地址的对应关系，并保存在各自的 ARP 表中。

## 六、思考题

（1）分别叙述各实验的记录结果并分析其原因。

（2）请画出 C 类地址的子网划分选择表。

（3）在 B 类网络中，能使用掩码 255.255.255.139 吗？为什么？

（4）说出地址和子网掩码的不同？

# 实验 4　交换机的基本配置

**【实际应用背景描述】**

（1）你是公司新来的网络管理员，公司要求你熟悉网络产品，公司采用的是全系列的锐捷网络产品，首先要求你登录交换机，了解掌握交换机的命令行操作。

（2）公司有部分主机网卡属于 10Mbps 网卡，传输模式为半双工，为了能实现主机之间的正常通信，现将和主机相连的交换机端口速率设置为 10Mbps，传输模式设为半双工，并开启该端口进行数据的转发。

（3）你是公司的新网管，第一天上班时，你必须掌握公司交换机的当前工作情况，通过查看交换机的系统信息和配置信息，了解公司的设备和网络环境。

## 一、实验目的

（1）熟练掌握网络互联设备——交换机的管理配置方法，了解带内管理与带外管理的区别。

（2）熟悉掌握锐捷网络设备的命令行管理界面。

（3）掌握交换机命令行各种配置模式的区别以及模式之间的切换。

（4）掌握交换机的基本配置方法。

## 二、实验设备（为每一实验小组提供如下实验设备）

（1）实验台设备：计算机两台 PC1 和 PC2。

（2）实验机柜设备：S2126（或者 S3550）交换机一台。

（3）实验工具及附件：网线测试仪一台，跳线若干。

## 三、实验基本原理及相关概念

（1）S2126G 交换机的管理方式：带内管理和带外管理。

- 带外管理方式：使用专用的配置线缆，将计算机的 COM 口与交换机的 Console 口连接，使用操作系统自带的超级终端程序登录到交换机，对交换机进行初始化配置。它不通过网络来管理配置交换机，不占用网络传输带宽，因此这种方式被称做带外管理。
- 带内管理方式：交换机在经过带外方式的基本配置后，就可以使用网络连接，通过网络对交换机进行管理配置，配置命令数据传输时，要通过网路线路进行，需要占用一定的网络带宽，浪费一定的网路资源，这种方式称为带内管理。

（2）交换机命令行操作模式：

- 用户模式：进入交换机后得到的第一个配置模式，该模式下可以简单查看交换机的软、

硬件版本信息，并进行简单的测试。用户模式提示符为：S2126G〉

- 特权模式：由用户模式进入的下一级模式，在该模式下可以对交换机的配置文件进行管理，查看交换机的配置信息，进行网络的测试和调试等操作。特权模式显示符为：S2126G#
- 全局配置模式：属于特权模式的下一级模式，该模式下可以配置交换机的全局性参数（如主机名、登录信息等）。在该模式下可以进入下一级的配置模式，对交换机的具体功能进行配置。全局模式提示符为：S2126G（config）#
- 端口配置模式：属于全局模式的下一级模式，该模式下可以对交换机的端口进行参数配置。端口模式提示符为：S2126G（config-if）#

（3）交换机命令行支持获取帮助信息、命令的简写、命令的自动补齐、快捷键功能等。

## 四、实验拓扑图（如图 9-22 所示）

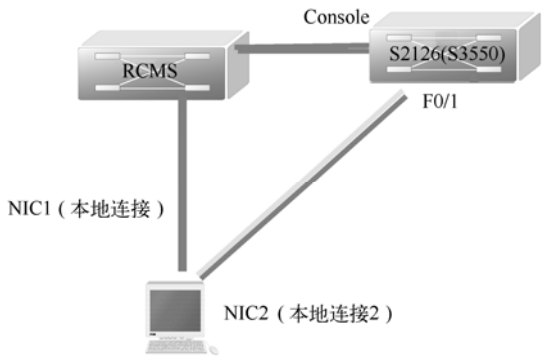



图 9-22　交换机基本配置实验拓扑图

## 五、实验项目及具体步骤

（1）掌握本组实验网络设备的配置管理界面的进入方法并记录实验操作结果。

**【步骤 1】**在计算机桌面上打开 IE 浏览器，在地址栏内输入实验室网络设备管理配置用 URL 地址，打开配置管理界面如图 9-23 所示。使用的地址如下。

- `http://192.168.1.10:8080`　（1～4 实验小组用）
- `http://192.168.1.20:8080`　（5～8 实验小组用）
- `http://192.168.1.30:8080`　（9～12 实验小组用）

**注意：**实验室环境中使用了 3 台锐捷网络公司研制开发的 RCMS 实验室管理控制器统一管理配置所有学生实验用网络设备，故存在 3 个访问地址。

**【步骤 2】**单击实验小组所属的网络设备图标，打开命令窗口，再按回车键，正常情况下应进入到相应设备的用户配置模式下，如图 9-24 所示。如果不能进入用户配置模式，则检查计算机的 IP 地址是否设置正确，要确保主机 IP 地址与地址栏内使用的管理设备的 IP 地址同属于一个子网，并使用 ping 命令测试本地主机与地址栏内 IP 地址所属设备能否连通。


图 9-23　网络设备管理配置界面

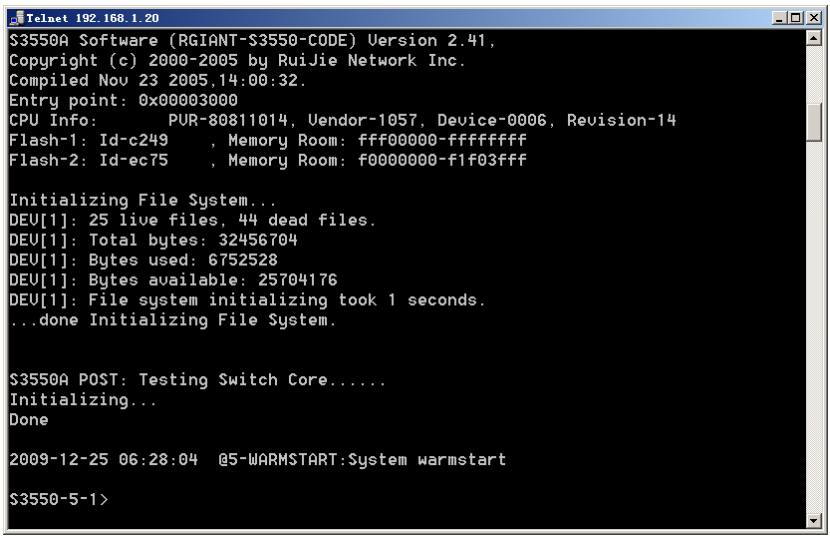



图 9-24　交换机用户配置模式界面

（2）交换机的基本配置。

**【步骤 1】**从用户模式开输入以下命令，练习交换机配置操作模式的进入与切换。

```
➢ S2126G〉enable                                    ! 进入特权模式
➢ S2126G #configure terminal                        ! 进入全局配置模式
➢ S2126G (config)#
➢ S2126G (config)#interface fastethernet 0/1        ! 进入 f0/1 的接口配置模式
➢ S2126G (config-if)#
➢ S2126G (config-if)#exit                           ! 退回到上一级操作模式
```

```
S2126G (config)#
S2126G (config-if)#end                          ! 直接退回到特权模式
S2126G #exit
S2126G〉                                         ! 返回最初的用户模式
```

注意：重复以上的操作步骤，反复练习。

【步骤 2】命令行帮助信息的使用练习：

```
S2126G〉？                ! 显示当前模式下所有可执行的命令
S2126G〉en？              ! 显示当前模式下所有以 en 开头的命令
S2126G〉show  ？          ! 显示 show 命令后可以使用的参数
```

【步骤 3】命令的简写：在特权模式下使用下面的命令形式进入到全局配置模式。

```
S2126G #conf  ter                ! 可代替 S2126G # configure terminal
S2126G (config)#end
S2126G #
```

【步骤 4】命令的自动补齐：在特权模式下，输入 conf 后按 Tab 键，则自动补齐命令 configure，再按一次 Tab 键，则自动补齐命令为 configure terminal。

```
S2126G #conf  Tab 键
S2126G #configure Tab 键
S2126G #configure terminal
```

【步骤 5】命令的快捷键功能：在接口配置模式下，使用 Ctrl+Z 组合键直接退回特权配置。

```
S2126G #configure terminal
S2126G (config)#interface  fastethernet 0/1
S2126G (config-if)# ctrl+z        ! 退回特权模式
S2126G #
```

（3）交换机的全局配置。

【步骤 1】配置交换机设备名称：改变交换机的名称为 switch，再改回原来的名字 S2126G。

```
S2126G# configure terminal
S2126G（config）# hostname  switch
Switch(config)# hostname S2126G
S2126G（config）#end
S2126G#exit
S2126G>
```

【步骤 2】配置交换机端口参数。

```
S2126G > enable
```

```
S2126G # configure terminal
S2126G (config)# interface fastethernet 0/3
S2126G(config-if)# speed 10
S2126G(config-if)# duplex half
S2126G(config-if)# no shutdown
S2126G(config-if)# end
S2126G #
```

【步骤 3】查看交换机端口的配置信息。

```
S2126G # show interface  fastethernet 0/3
```

（4）在交换机上配置管理 IP 地址。

【步骤 1】参照下列操作步骤进行配置。

```
S2126〉enable                          ! 进入特权模式
S2126#configure terminal              ! 进入全局配置模式
S2126(config)#hostname switchA        ! 配置交换机名称为"switchA"
switchA(config)#interface vlan 1      ! 进入交换机管理接口配置模式
switchA(config-if)#ip   address 192.168.0.138   255.255.255.0 ！ 配置交换机管理接口 IP 地址
switchA(config-if)#no shutdown        ! 开启交换机管理接口
switchA(config-if)#end
S2126#
```

【步骤 2】验证测试：验证交换机管理 IP 地址已经配置和开启。

```
switchA#show interface vlan 1 ! 验证交换机管理 IP 地址已经配置，管理接口已经开启
```

【步骤 3】使用 ping 命令测试验证网络的连通性，从主机可以到达 192.168.0.138。

【步骤 4】配置交换机远程登录密码为 student。（注意：必须具有最高级用户权限）

```
switchA(config)#enable secret level 1 0 student  ！1 表示远程登录，0 表示是以密文形式传输，并设置交换机远程登录密码为"student"
```

【步骤 5】验证从 PC 的命令行窗口可以使用 Telnet 客户端程序，通过网线远程登录到交换机上，实现带内管理，具体操作如图 9-25、图 9-26 所示。

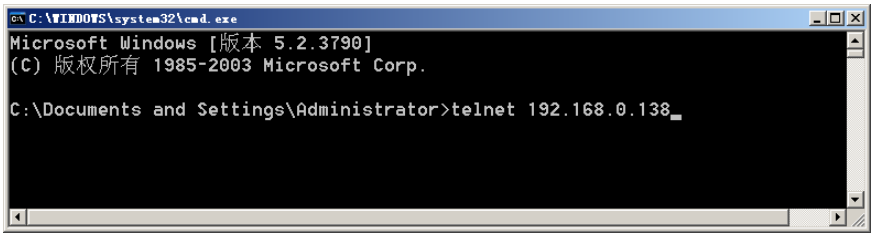



图 9-25　远程登录交换机

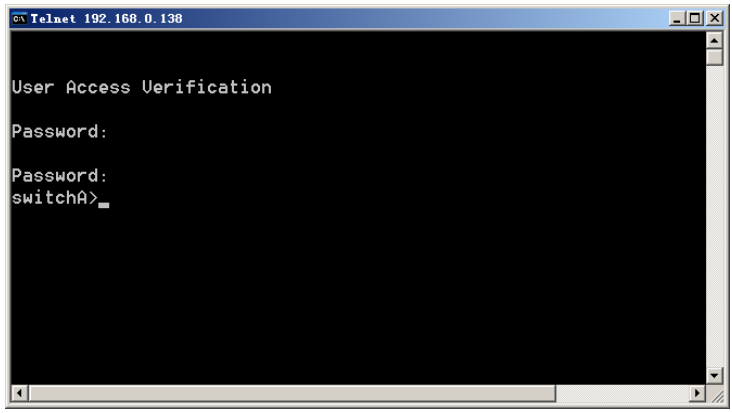



图 9-26　进入用户配置模式实现带内管理

（5）配置交换机特权模式密码。（注意：必须具有最高级用户权限）

```
➢ switchA(config)#enable secret level 15 0 student ! 15 表示特权模式，0 表示是以密文形式传输，并设置交换机特权模式密码为"student"
```

（6）交换机配置文件的管理。

- 保存配置：将当前运行的参数保存到 Flash 中，用于系统初始化时初始化参数。

```
➢ Switch#copy running-config startup-config
➢ Switch#write memory
➢ Switch#write
```

- 删除当前配置：在配置命令前加 no，如删除 IP 地址配置信息则用如下配置：

```
➢ switch(config-if)# no ip address
```

- 查看配置文件内容。

```
➢ Switch#show configure              ! 查看保存在 Flash 里的配置信息
➢ Switch#show running-config         ! 查看 RAM 里当前生效的配置
➢ Switch#show version                ! 查看交换机的版本信息
```

- 验证交换机配置已保存。

```
➢ switchA#show configure             ! 验证交换机配置已保存
```

**注意：**

交换机的管理接口默认是关闭的（shut down），因此在配置管理接 interface vlan 1 的 IP 地址后须用命令“no shutdown”开启该接口。

## 六、思考题

（1）主机与交换机之间通过 Telnet 建立连接时，采用的是交换机的什么接口？这时使用的双绞线是直连线还是交叉线？

（2）观察你所配置的交换机的型号，说出其为几层交换机。

（3）如果不使用 RCMS 管理系统，如何实现带外管理，使用什么线缆，能否进行远程配置？

# 实验 5　交换机端口隔离

**【实际应用背景描述】**

假设你所用的交换机是宽带小区城域网中的 1 台楼道交换机，住户不希望他们之间能够相互访问，现要实现各家各户的端口隔离。现在住户 PC1 计算机连接在交换机的 f0/1 口，住户 PC2 计算机连接在交换机的 f0/2 口。

## 一、实验目的

（1）熟练掌握网络互联设备——交换机的基本配置方法。

（2）理解和掌握 PORT VLAN 的配置方法。

## 二、实验设备（为每一实验小组提供如下实验设备）

（1）实验台设备：计算机两台 PC1 和 PC2（或者 PC4 和 PC5）。

（2）实验机柜设备：S2126（或者 S3550）交换机一台。

（3）实验工具及附件：网线测试仪一台，跳线若干。

## 三、实验相关知识

（1）VLAN（Virtual Local Area Network，虚拟局域网），是指在一个物理网段内，进行逻辑的划分，划分成若干个虚拟局域网。其最大的特性是不受物理位置的限制，可以进行灵活的划分。VLAN 具备一个物理网段所具备的特性，相同的 VLAN 内的主机可以相互直接访问，不同的 VLAN 间的主机之间互相访问必须经由路由设备进行转发，广播包只可以在本 VLAN 内进行传播，不能传输到其他 VLAN 中。

（2）PORT VLAN 是实现 VLAN 的方式之一，PORT VLAN 是利用交换机的端口进行 VLAN 的划分，一个普通端口只能属于一个 VLAN。

## 四、实验所用拓扑图（如图 9-27 所示）


图 9-27　交换机端口隔离实验拓扑图

注意：实验时按照拓扑图进行网络的连接，注意主机和交换机连接的端口。

## 五、实验内容及操作步骤

（1）启动 IE 浏览器打开实验网络设备的配置管理界面。（注意：具体步骤参照实验三）

（2）按照图 9-28 所示的拓扑完成实验设备物理连接，实现两台主机的互联互通，确保在未划分 VLAN 前两台 PC 是可以通信的（即交换机 F0/1 和 F0/2 端口间是可以通信的）。（注意：具体步骤参照实验二）

（3）创建 VLAN，划分端口实现端口隔离。

【步骤 1】从交换机的用户配置模式开始按下列方法进行配置操作：

```
S2126G〉enable                          ！进入特权模式
S2126G # configure terminal            ！进入全局配置模式
S2126G (config)#vlan 10                ！创建 VLAN 10
S2126G (config-vlan)#name  test10      ！将 VLAN 10 命名为 Test10
S2126G (config-vlan)#exit              ！退回到上一级操作模式
S2126G (config)#vlan 20                ！创建 VLAN 20
S2126G (config-vlan)#name  test20      ！将 VLAN 20 命名为 Test20
S2126G (config-vlan)#end               ！直接退回到特权模式
S2126G #
```

【步骤 2】验证测试：查看 VLAN 配置信息。

```
S2126G #show vlan                      ！查看已配置的 VLAN 信息
```

注意：默认情况下，所有的接口都属于 VLAN 1

【步骤 3】将接口 F0/1 和 F0/2 分别分配到 VLAN 10 和 VLAN 20，并记录实验结果。

```
S2126G# configure terminal
S2126G（config）#interface fastethernet 0/1
S2126G（config-if）#switchport access vlan 10
S2126G（config-if）#exit
S2126G（config）#interface fastethernet 0/2
S2126G（config-if）#switchport access vlan 20
S2126G（config-if）#exit
```

【步骤 4】验证配置并记录实验结果：

```
S2126G #show vlan
```

【参考配置信息】

```
Vlan name    status    ports

1 default  active     Fa0/3,Fa0/4,Fa0/5
```

```
                                                    ……
Fa0/22, Fa0/23   Fa0/24
10  test10    active  Fa0/1   ! 划入端口 F0/
20  test20    active  Fa0/2   ! 划入端口 F0/2
```

【步骤 5】测试验证，原来可以通信的两台主机，现在 ping 不通，并记录实验结果。

（4）查看交换机端口的配置信息：

```
➢  S2126G # show interface  fastethernet 0/1  switchport
```

（5）查看验证交换机配置信息：

```
➢  switchA#show running-config
```

注意：

- 交换机所有端口在默认情况下属于 access 端口，可直接将端口加入某一 VLAN，利用 switchport mode access/trunk 命令可以更改端口的 VLAN 模式。
- VLAN1 属于系统默认的 VLAN，不可以被删除。
- 删除某个 VLAN，应使用 NO 命令。例如：switch（config）#no VLAN 10
- 删除某个 VLAN 时，应先将属于该 VLAN 的端口加入到别的 VLAN 中，再删除。否则被删除的 VLAN 内的分配端口会自动恢复到系统默认的 VLAN1 中。

## 六、分析与思考

（1）观察配置的交换机的型号，指出其为几层交换机。

（2）VLAN 的划分方法有哪些？基于端口的 VLAN 的划分的优缺点是什么？

（3）一个交换机端口，能否属于不同的 VLAN？

# 实验 6　路由器的基本配置

【实际应用背景描述】

（1）你是公司新来的网络管理员，要求熟悉网络产品，公司采用的是全系列的锐捷网络产品，首先要求你登录路由器，了解掌握路由器的命令行操作。

（2）公司有多台路由器，为了进行区分和管理，要求你进行路由器设备名的配置，配置路由器登录时的描述信息。

（3）你在一家网络公司就职，负责组建一个省级广域网络。现项目经理要求你根据实际网络需要，对路由器的端口配置基本的参数。

## 一、实验目的

（1）熟练掌握网络互联设备——路由器的管理配置方法，了解带内管理与带外管理的区别。

（2）熟悉掌握锐捷网络设备的命令行管理界面。
（3）掌握路由器的命令行各种配置模式的区别，以及模式之间的切换。
（4）掌握路由器的基本配置方法。

## 二、实验设备（为每一实验小组提供如下实验设备）

（1）实验台设备：计算机两台 PC1 和 PC2。
（2）实验机柜设备：R1762 路由器两台。
（3）实验工具及附件：网线测试仪一台，跳线若干。

## 三、实验技术原理

（1）路由器的管理方式：带外管理和带内管理方式。

- 带外管理方式：使用专用的配置线缆，将计算机的 COM 口与路由器的 Console 口连接，使用操作系统自带的超级终端程序登录到路由器，对路由器进行初始化配置。它不通过网络来管理配置路由器，不占用网络传输带宽，因此这种方式被称为带外管理。特点是需要特殊的配置线缆，只能进行近距离配置。第一次配置路由器时必须利用 Console 口进行配置，使其支持 Telnet 远程管理。
- 带内管理方式：路由器在经过带外方式的基本配置后，就可以使用网络连接，通过网络对路由器进行管理配置，配置命令数据传输时，要通过网络线路进行，需要占用一定的网络带宽，浪费一定的网络资源，这种方式称为带内管理方式。其特点是可以实现远程管理。

（2）路由器命令行操作模式：

- 用户模式：进入路由器后得到的第一个配置模式，该模式下可以简单查看路由器的软、硬件版本信息，并进行简单的测试。用户模式提示符为：R1762-1〉
- 特权模式：由用户模式进入的下一级模式，在该模式下可以对路由器的配置文件进行管理，查看路由器的配置信息，进行网络的测试和调试等。特权模式显示符为：R1762-1 #
- 全局配置模式：属于特权模式的下一级模式，该模式下可以配置路由器的全局性参数（如主机名、登录信息等）。在该模式下可以进入下一级的配置模式，对路由器的具体功能进行配置。全局模式提示符为：R1762-1（config）#
- 端口配置模式：属于全局模式的下一级模式，该模式下可以对路由器的端口进行参数配置。端口模式提示符为：R1762-1（config-if）#

（3）路由器命令行支持获取帮助信息、命令的简写、命令的自动补齐、快捷键功能等。

（4）锐捷路由器接口 FASTETHERNET 默认情况下是 10/100Mbps 自适应端口，双工模式也为自适应，并且在默认情况下，路由器物理端口处于关闭状态。所以端口配置一般不配置传输速率和工作模式，但必须开启端口。

（5）路由器提供广域网接口（Serial 高速同步串口），使用 V.35 线缆连接广域网接口链路，

在广域网连接时一端为 DCE（数据通信设备），一端为 DTE（数据终端设备）。要求必须在 DCE 端配置时钟频率（clock rate）才能保证链路的连通。

（6）在路由器的物理端口可以灵活配置带宽，但最大值为该端口的实际物理带宽。

## 四、实验注意事项及要求

（1）实验中严禁在设备端口上随意插拔线缆，如果确实需要应向老师说明征求许可。
（2）以电子文档形式提交实验报告。
（3）将路由器的配置文档、验证计算机的 TCP/IP 配置信息保存。
（4）将路由器的配置信息以图片的形式保存到实验报告中。

## 五、实验用拓扑图（如图 9-28 所示）

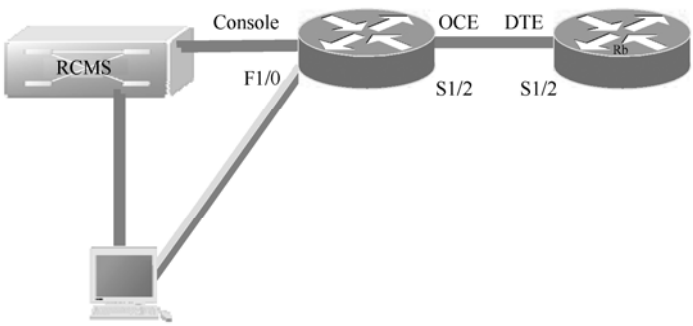



图 9-28　路由器的基本配置实验拓扑图

## 六、实验具体步骤及实验结果记录

（1）启动 IE 浏览器打开实验网络设备的配置管理界面。（注意：具体步骤参照实验三）
（2）按照图 9-28 所示的拓扑完成实验设备物理连接。
（3）路由器的配置：

**【步骤 1】**命令行操作模式的进入和退出（参考配置如下）：

```
➢ R1762-1〉enable                                    ! 进入特权模式
➢ R1762-1 # configure terminal                       ! 进入全局配置模式
➢ R1762-1 (config)#
➢ R1762-1 (config)#interface fastethernet 1/0        ! 进入接口的配置模式
➢ R1762-1 (config-if)#
➢ R1762-1 (config-if)#exit                           ! 退回到上一级操作模式
➢ R1762-1 (config)#
➢ R1762-1 (config-if)#end                            ! 直接退回到特权模式
➢ R1762-1 #
```

```
R1762-1 #conf  ter                                    ! 命令的简写
R1762-1 (config)#end
R1762-1 #exit
R1762-1>
```

【步骤 2】路由器的设备名称的配置(属于路由器全局配置内容)：

```
R1762-1〉enable
R1762-1# configure terminal
R1762-1（config）#hostname  routerA
routerA(config)#hostname R1762-1
R1762-1 (config)#end
R1762-1 #exit
R1762-1>
```

【步骤 3】路由器每日提示信息的配置（属于路由器全局配置内容)：

```
R1762-1 > enable
R1762-1 # configure terminal
R1762-1 (config)# banner motd &              ！ 配置每日提示信息，&为终止符
Enter TEXT message.  End with the character '&'.
Welcom to routerA ,if you are admin ,you can config it
if you are not amdin ,please exit
&                                            ! 输入&符号终止输入
```

【步骤 4】验证测试：

```
R1762-1（config）#end
R1762-1#exit
Press return to get started
Welcome to RouterA,if you are admin,you can config it.
If you are not admin, please exit.
R1762-1>
```

注意：

（1）配置设备名称的有效字符是 22 个字符。

（2）配置每日提示信息时，终止符只能放在描述文本最后。

【步骤 5】在两个路由器上完成端口配置，实现路由器之间的连通。

- 路由器 A 端口参数的配置。

```
R1762-1 #  configure terminal                ! 进入全局配置模式
R1762-1 (config)#hostname Ra
R1762-1 (config)#interface serial 1/2        ! 进入 s1/2 的接口配置模式
R1762-1 (config-if)#ip address 1.1.1.1 255.255.255.0 ! 配置端口 IP
```

```
➢ R1762-1 (config-if)#clock rate 64000          ! 在 DCE 接口上配置时钟频率
➢ R1762-1 (config-if)#bandwidth 512             ! 配置端口的带宽速率为 512KB
➢ R1762-1 (config-if)#no shutdown               ! 开启该端口，使端口转发数据
➢ R1762-1 #                                   ! 配置带宽时，以 K 为单位
```

- 路由器 B 端口参数的配置。

```
➢ R1762-2 #  configure terminal                 ! 进入全局配置模式
➢ R1762-2 (config)#hostname Rb
➢ R1762-2 (config)#interface serial 1/2         ! 进入 s1/2 的接口配置模式
➢ R1762-2 (config-if)#ip address 1.1.1.2 255.255.255.0 ! 配置端口 IP
➢ R1762-2 (config-if)#bandwidth 512             ! 配置端口的带宽速率为 512KB
➢ R1762-1 (config-if)#no shutdown               ! 开启该端口，使端口转发数据
➢ R1762-1 #                                     ! 配置带宽时，以 K 为单位
```

【步骤 6】验证配置：

```
➢ ra#ping 1.1.1.2    ! 在 RA 上 ping 对端 rb serial 1/2 接口的 ip
```

【参考配置信息】

```
Sending 5, 100-byte ICMP Echoes to 1.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/30/30 ms
ra#
```

【步骤 7】查看 Ra 路由器端口的配置信息：

```
➢ Ra # show interface  serial 1/2       ! 查看 Ra s1/2 接口的状态
```

【步骤 8】查看 Rb 路由器端口的配置信息：

```
➢ Rb # show interface  serial 1/2       ! 查看 Rb S1/2 接口的状态
```

【步骤 9】查看路由器 IP 协议相关的配置信息：

```
➢ rb#show ip interface serial 1/2       !  查看该端口的 IP 协议相关属性
```

注意：

（1）路由器默认情况下是关闭的，需要 no shutdown 开启端口。

（2）Serial 接口正常的端口速率最大是 2.048MZ（2000KB）。

（3）Show interface 和 show ip interface 之间的区别。

【步骤 10】在路由器的 fastethernet 端口上配置 IP 地址。

```
➢ R1762〉enable                          ! 进入特权模式
➢ R1762#configure terminal              ! 进入全局配置模式
➢ R1762(config)#hostname ROUTERA        ! 配置路由器名称为"ROUTERA"
```

```
➢ switchA(config)#interface fastethernet 1/0   ！进入路由器 f1/0 接口
➢ switchA(config-if)#ip address 192.168.100.1  255.255.255.0 ！配置路由器 f1/0 接口 IP 地址
➢ switchA(config-if)#no shutdown        ！开启路由器 f1/0 接口
```

【步骤 11】验证测试 1：验证路由器管理 IP 地址已经配置和开启。

使用 ping 命令测试验证网络的连通性，从主机可以到达 192.168.100.1 管理地址。

```
➢ c:\>ping 192.168.100.1
```

【参考配置信息】

```
Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

【步骤 12】验证测试 2：验证从 PC 可以通过网络远程登录到路由器上，配置正确会显示欢迎信息，输入正确的远程登录密码后进入用户配置模式，如图 9-29 所示。

```
➢ c:\>telnet 192.168.100.1  ！从 PC 登录到路由器上
```

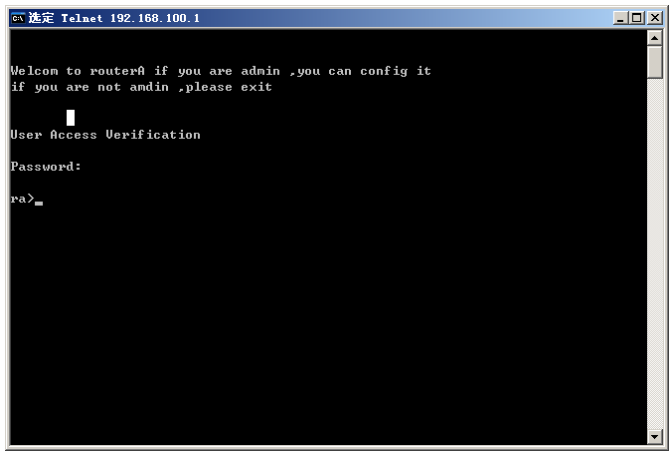



图 9-29　远程登录管理配置路由器

【步骤 13】查看路由器各项配置信息：

```
➢ rouerA# show version              ！查看路由器的版本信息
➢ rouerA# show ip route             ！查看路由器路由表信息
```

```
➢ routerA#show running-config        ! 查看路由器当前生效的配置信息
```

【步骤 14】路由器配置文件的管理。

- 保存配置（略）。将当前运行的参数保存到 Flash 中用于系统初始化时初始化参数。

```
➢ Switch#copy running-config startup-config
➢ Switch#write memory
➢ Switch#write
```

- 删除配置。

```
➢ 永久性的删除 Flash 中不需要的文件
➢ 使用命令 delete flash:config.text（注意：仅 15 级用户可以使用）
➢ 删除当前的配置：  在配置命令前加 no
➢ 例：switch(config-if)# no ip address
```

- 查看配置文件内容。

```
➢ Switch#show startup-config        查看保存在 Flash 里的配置信息
➢ Switch#show running-config        查看 RAM 里当前生效的配置
➢ Switch#show version               查看路由器的版本信息
➢ Show mac-address-table            查看路由器当前生效的配置信息
```

- 验证测试：验证路由器配置已保存。

```
➢ switchA#show startup-config        ! 验证路由器配置已保存
```

注意：

（1）路由器的管理接口默认一般是关闭的（Shutdown），因此在配置接口（Interface）的 IP2 地址后须用命令“no shutdown”开启该接口。

（2）DCE 端要配置时钟频率。

## 七、分析与思考

（1）主机与路由器之间通过 Telnet 建立连接时，采用路由器的什么口？这时使用的是双绞线的直连线还是交叉线？

（2）观察你所配置的路由器的型号，说出它有几个端口？分别是哪些端口？

# 实验 7　静态路由的配置

【实际应用背景描述】

设校园网通过 1 台路由器连接到校园外的另一台路由器上，现要在路由器上做适当的配置，实现校园网内部主机与校园网外部主机的相互通信。

## 一、实验目的

掌握路由器静态路由的基本配置方法。

## 二、实验设备（为每一实验小组提供如下实验设备）

（1）实验台设备：计算机两台 PC1 和 PC2。
（2）实验机柜设备：R1762 路由器两台。
（3）实验工具及附件：网线测试仪一台，跳线若干。

## 三、实验内容及技术原理

（1）路由器属于网络层设备，能够根据 IP 包头的信息，选择一条最佳路径，将数据包转发出去，实现不同网段的主机之间的互相访问。

（2）路由器是根据路由表进行选路和转发的。而路由表就是由一条条的路由信息组成，路由表的产生方式一般有 3 种：

- 直连路由：给路由器接口配置一个地址，路由器自动产生本接口 IP 所在网段的路由信息。
- 静态路由：在拓扑结构简单的网络中，管理员通过手工的方式配置本路由器未知网段的路由信息，从而实现不同网段之间的连接。
- 动态路由：路由器通过学习路由协议自动产生的路由信息。

## 四、实验注意事项及要求

（1）将路由器的配置文档、验证计算机的 TCP/IP 配置信息保存。
（2）将路由器的配置信息以图片的形式保存到实验报告中。

## 五、实验用拓扑图（如图 9-30 所示）

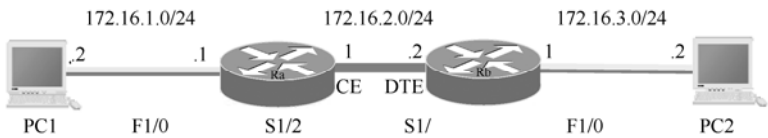



图 9-30　静态路由配置

注意：普通路由器和主机直接连接时，需要使用交叉线，在 R1762 的以太网接口支持 MDI/MDIX，使用直连线也可以连通。

## 六、实验具体步骤及实验结果记录

（1）测试验证本组实验网络设备的配置管理界面的进入方法（参照实验三）。

（2）按照实验拓扑图完成实验设备的物理连接，并进行简单的测试，保证连接无误。

（3）路由器的配置。

**【步骤 1】**在路由器 Ra 上配置接口的 IP 地址和串口上的时钟频率。

```
RA〉enable
RA # configure terminal
RA (config)#
RA (config)#interface fastethernet 1/0
RA (config-if)# ip address 172.16.1.1 255.255.255.0
RA (config-if)# no shutdown
RA (config-if)# exit
RA (config)#interface serial 1/2
RA (config-if)# ip address 172.16.2.1 255.255.255.0
RA (config-if)# clock rate 64000
RA (config-if)# no shutdown
RA (config-if)# end
```

**【步骤 2】**验证路由器接口的配置。

```
RA #show ip interface brief
ra#show ip interface brief
Interface              IP-Address(Pri)    OK?        Status
serial 1/2             172.16.2.1/24      YES        UP
serial 1/3             no address         YES        DOWN
FastEthernet 1/0       172.16.1.1/24      YES        UP
FastEthernet 1/1       no address         YES        DOWN
```

**注意：**查看接口状态。

```
RA #show  interface serial 1/2
ra#show  interface serial 1/2
```

**【步骤 3】**在路由器 Ra 上配置静态路由。

```
RA (config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2
```

或者：

```
RA (config)#ip route 172.16.3.0 255.255.255.0 serial 1/2
```

**【步骤 4】**验证测试：验证 Ra 上的静态路由配置。

```
RA #show  ip  route
```

【参考配置信息】

```
Codes:  C - connected, S - static,  R - RIP B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default
Gateway of last resort is no set
C    172.16.2.0/24 is directly connected, serial 1/2
C    172.16.2.1/32 is local host.
S    172.16.3.0/24 [1/0] via 172.16.2.2
```

【步骤 5】在路由器 Rb 上配置接口的 IP 地址。

```
➢ Rb〉enable
➢ Rb # configure terminal
➢ Rb (config)# interface fastethernet 1/0
➢ Rb (config-if)# ip address 172.16.3.1 255.255.255.0
➢ Rb (config-if)# no shutdown
➢ Rb (config-if)# exit
➢ Rb (config)#  interface serial 1/2
➢ Rb (config-if)# ip address 172.16.2.2 255.255.255.0
➢ Rb (config-if)#  no shutdown
➢ Rb (config-if)# end
```

【步骤 6】验证路由器接口的配置。

```
➢ Rb #show ip interface brief
➢ RA #show  interface serial 1/2
```

【步骤 7】在路由器 Rb 上配置静态路由。

```
Rb(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

或者：

```
Rb(config)#ip route 172.16.1.0 255.255.255.0 serial 1/2
```

验证测试：验证 Rb 上的静态路由配置。

```
Rb #show  ip  route
```

【步骤 8】测试网络的互联互通性。

从 PC1 ping PC2

从 PC2 ping PC1

记录实验结果：

**注意：**

（1）如果两台路由器通过串口直接互联，则必须在其中的一端设置时钟频率（DCE 端）。

（2）测试验证两台主机连通时，要正确设置主机的网关地址，应为与它连接的路由器的以太网端口的地址。

## 七、分析与思考

（1）主机与路由器的端口之间通过什么线缆连接？是直连线还是交叉线？

（2）两台路由器通过高速同步串口直接互联时，使用什么线缆？哪一端必须配置时钟频率？

# 实验 8　DHCP 服务器的安装与配置

**【实际应用背景描述】**

假设你是某小区的网络管理员，小区网络中计算机的网络地址采用的是动态分配的方式。你需要搭建一个 DHCP 的服务器，这样小区中的用户就不需要手工配置计算机的 IP 地址等信息，计算机可以自动从 DHCP 服务器上获得这些信息。

## 一、实验目的

（1）掌握 DHCP 服务器的安装与基本配置方法。

（2）掌握客户机自动获取 IP 地址的设置方法。

## 二、实验设备

（1）计算机两台。

（2）双绞线两根。

（3）交换机一台。

## 三、实验环境

（1）操作系统环境：服务器，Windows Server 2003

（2）客户机 Windows XP。

## 四、实验步骤

### 1．安装 DHCP 服务

【步骤 1】执行“开始”→设置→“控制面板”命令 ，打开添加或删除程序窗口，如图 9-31 所示。

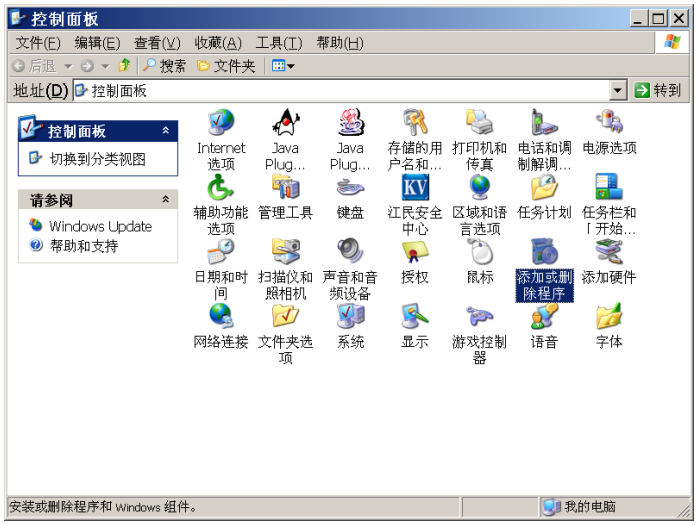



图 9-31　打开“添加或删除程序”窗口

【步骤 2】在“添加或删除程序”窗口中单击“添加删除 Windows 组件”项，打开“Windows 组件向导”对话框，如图 9-32 所示。

【步骤 3】在“Windows 组件向导”对话框中，选中“网络服务”项，然后单击“详细信息”按钮，打开“网络服务”对话框，如图 9-33 所示。

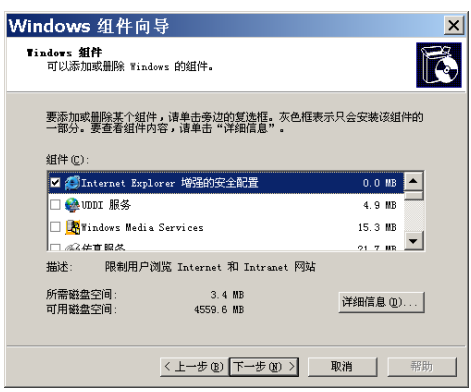



图 9-32　“Windows 组件向导”对话框

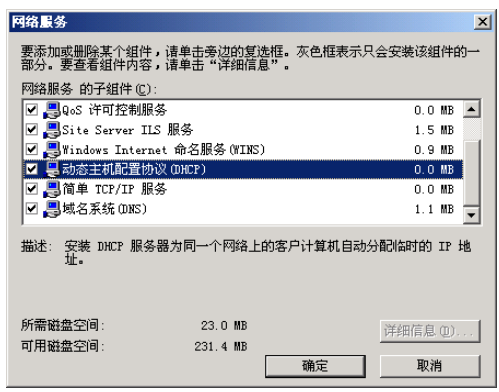



图 9-33　“网络服务”对话框

如果服务功能安装，则复选框被选中，否则选中“动态主机配置协议（DHCP）”对话框左侧的复选框，单击“确定”按钮后再单击“下一步”按钮，进行文件复制和安装操作。

【步骤 4】安装确认：安装完毕，可在计算机管理对话框中查看是否正确安装 DHCP，如

图 9-34 所示。

还可以在计算机管理窗口中的“服务与应用程序”中的服务列表中查看是否有“DHCP Server”服务功能，且状态为“已启动”，如图 9-35 所示。

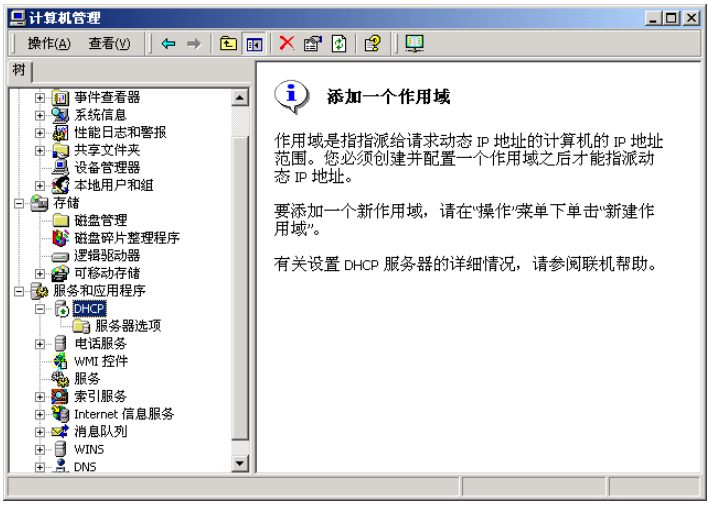



图 9-34　通过计算机管理窗口确认

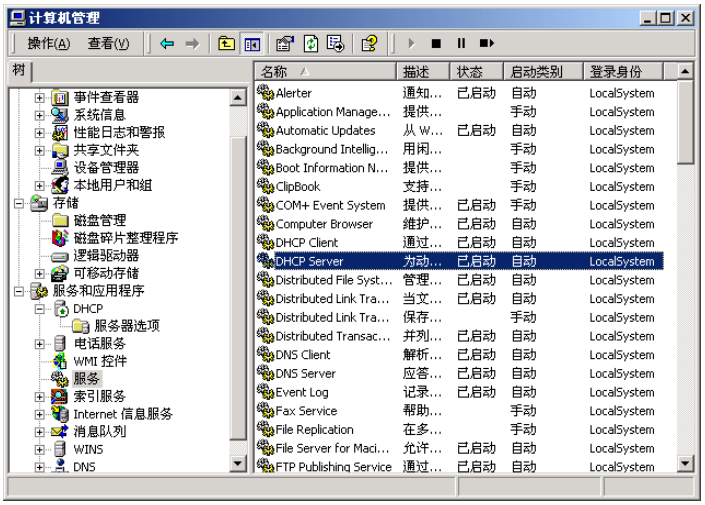



图 9-35　通过服务列表确认安装正常

### 2．服务器端 DHCP 安装后的配置

**【步骤 1】**使用控制面板里的 DHCP 管理工具进行配置：执行“开始”→“程序”→“管理工具”→“DHCP”命令，打开“DHCP 控制台”窗口，如图 9-36 所示。

**【步骤 2】**双击服务器图标，如图 9-37 所示。

**【步骤 3】**右击 w1 服务器可打开快捷菜单（操作菜单的命令），如图 9-38 所示选择“新建作用域”操作命令：打开新建作用域向导，如图 9-39 所示，单击“下一步”按钮，配置作用域名称，如图 9-40 所示。

**【步骤 4】**指定 IP 地址范围：单击“下一步”按钮，在 IP 地址范围内，输入准备分配给客户机的 IP 地址范围的起始地址和结束地址，设置好相应的子网掩码后，单击“下一步”按

钮，如图 9-41 所示。

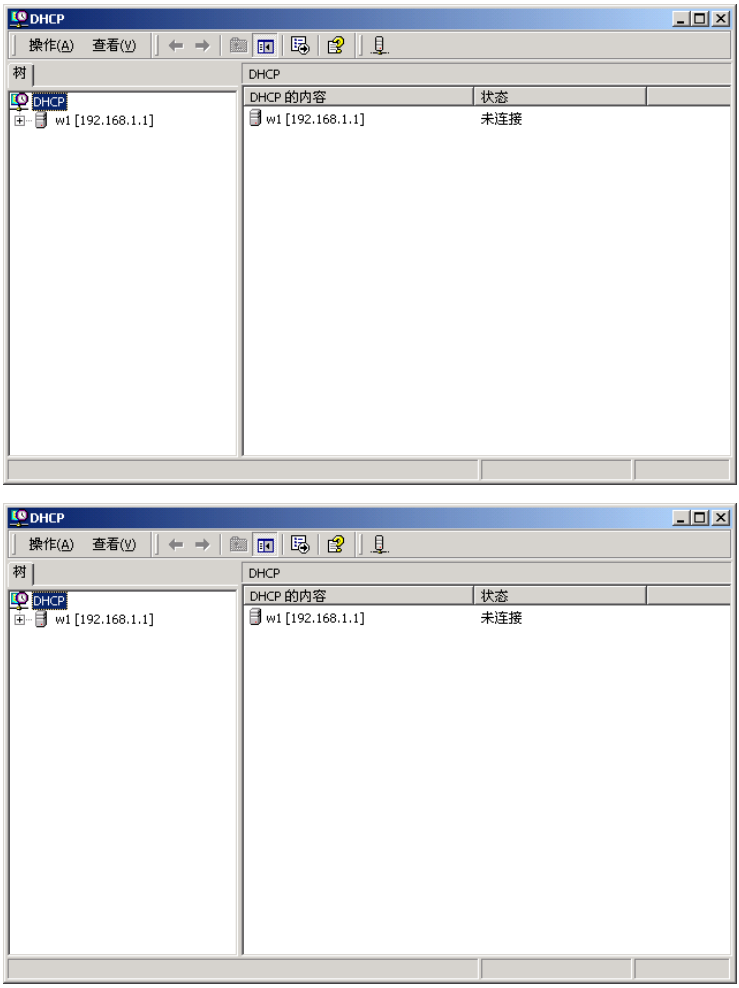



图 9-36　使用 DHCP 管理工具进行配置

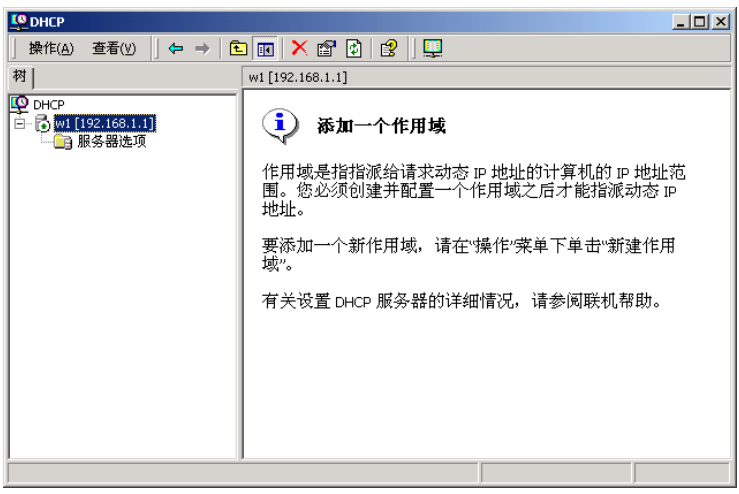



图 9-37　激活服务器

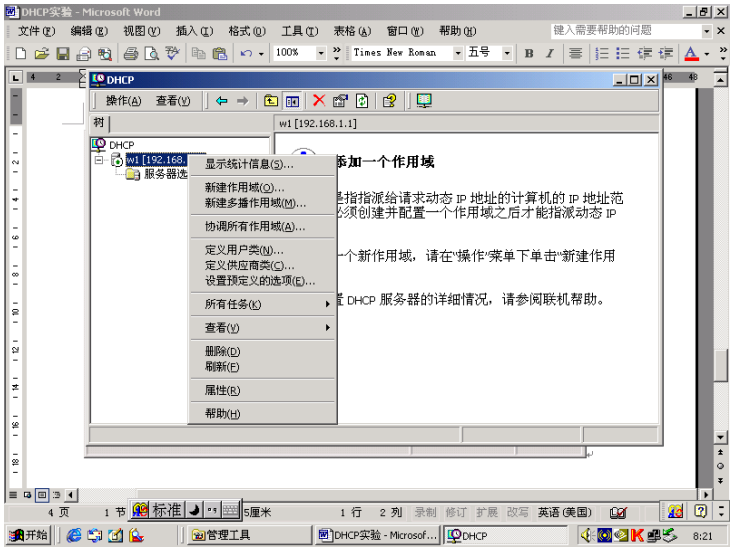



图 9-38　新建作用域

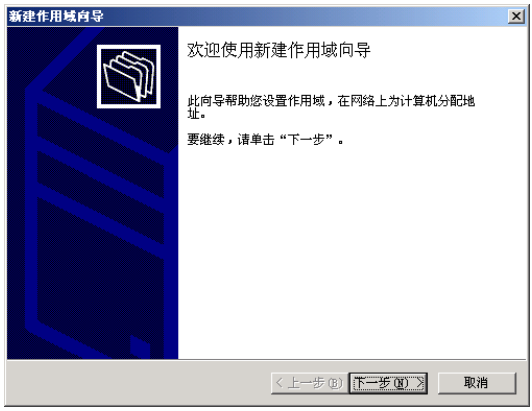



图 9-39　新建作用域向导图

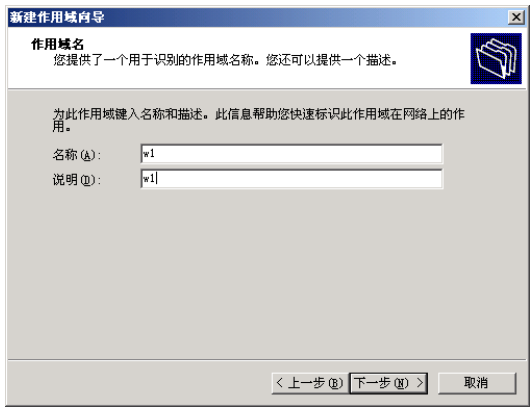



图 9-40　配置作用域名称

【步骤 5】添加排除地址范围：设置在上一步设置的 IP 地址范围中哪一小段 IP 地址范围不分配给客户机，在此做相应设置，单击“下一步”按钮，如图 9-42 所示。

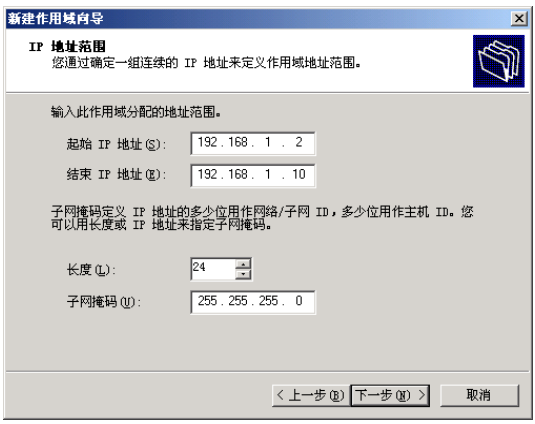



图 9-41　设置 IP 地址范围

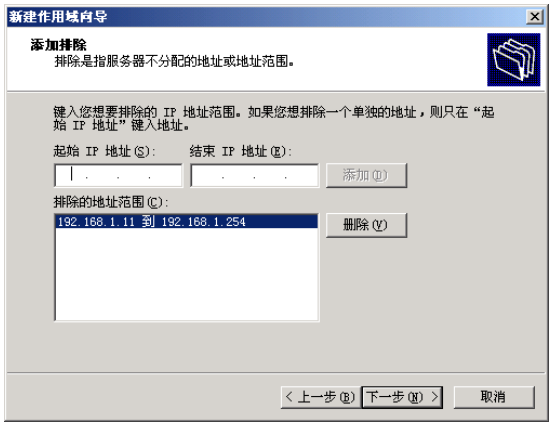



图 9-42　添加排除地址范围

【步骤 6】设定租约期限：设置客户机从 DHCP 服务器租用地址使用的时间长短，默认为 8 天，如图 9-43 所示。

【步骤 7】配置 DHCP 选项：选项包括默认网关、IP 地址、DNS 和 WINS 服务器地址等，选择“是，我想现在配置这些选项”项，如图 9-44 所示。

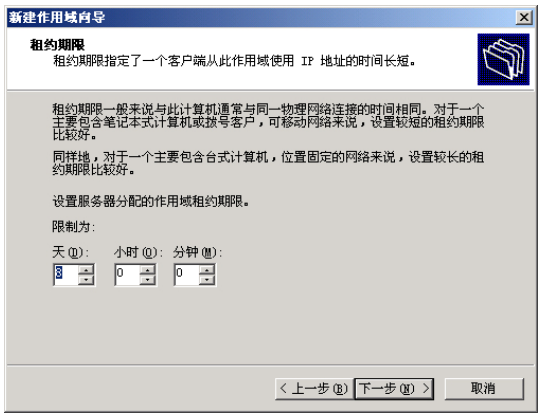



图 9-43　设定租约期限

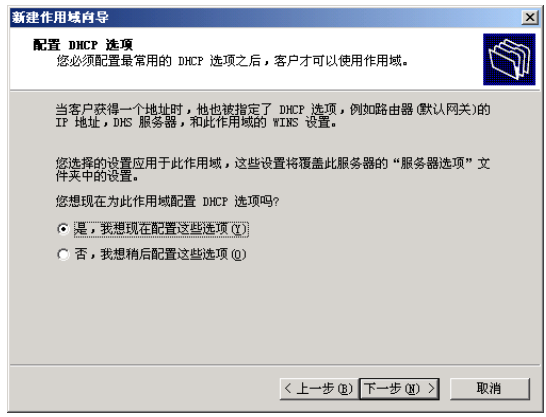



图 9-44　设定租约期限

【步骤 8】激活（启动）作用域，完成配置，如图 9-45、图 9-46 所示。

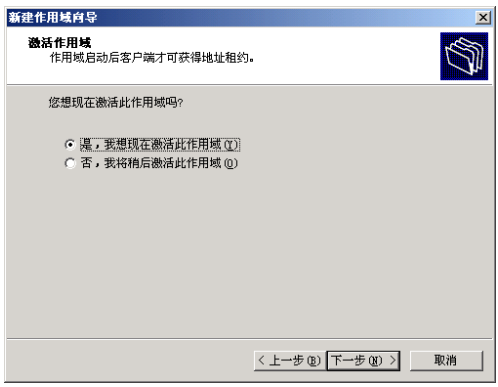



图 9-45　激活作用域

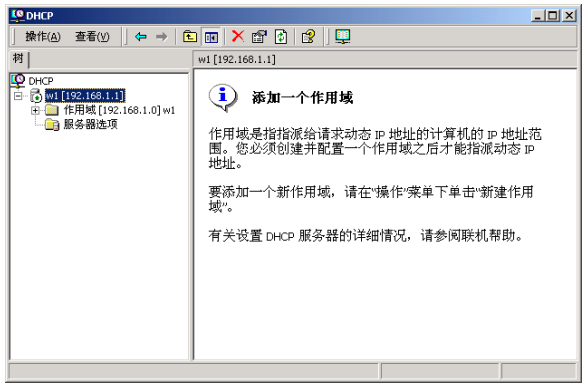



图 9-46　完成向导后的配置

### 3．DHCP 客户机的配置与测试

【步骤 1】DHCP 客户机的配置：

在 Windows 2000 Professional/xp 客户机桌面上，打开“本地连接 属性”对话框，如图 9-47 所示。

【步骤 2】在“本地连接 属性”对话框中选择“Internet 协议（TCP/IP）”，再选择“属性”，打开“Internet 协议（TCP/IP）属性”对话框，在该对话框中选择“自动获得 IP 地址”选项和“自动获得 DNS 服务器地址”选项，如图 9-48 所示。

【步骤 3】DHCP 客户机的测试：DHCP 客户机检查获得 IP 地址及其他选项的方法：

在命令提示符方式下，利用 Ipconfig 命令检查 IP 地址的获得：利用“Ipconfig/all”命令查看详细的 IP 设置（包括网卡的物理地址），如图 9-49 所示。


图 9-47　“本地连接 属性”对话框

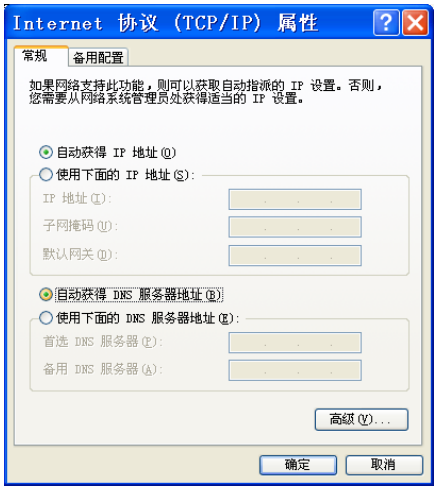



图 9-48　“Enternet 协议（TCP/IP）属性”对话框

使用“Ipconfig/release”命令可释放获得的 IP 地址；使用“Ipconfig/renew”命令重新获得地址。

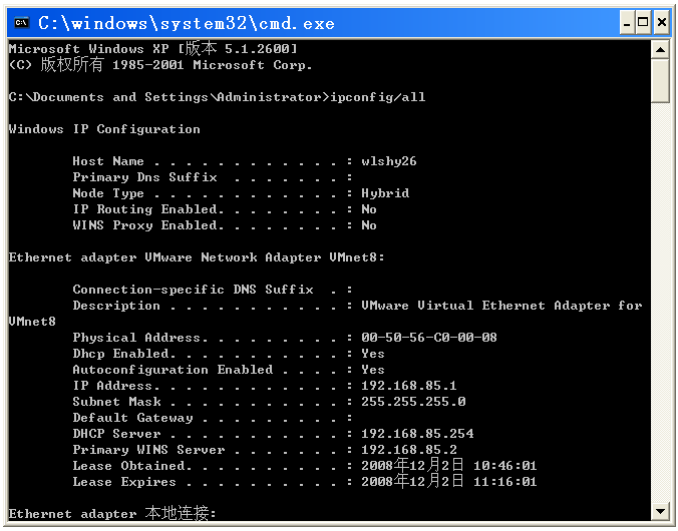



图 9-49　检查 TCP/IP 配置

### 4．从服务器端进行验证

【步骤 1】在服务器上使用 ping 命令测试到客户端的联通性：ping 192.168.1.2　-t，如图 9-50 所示。

【步骤 2】在 DHCP 管理控制台窗口查看：地址池、租约信息、服务器选项等信息。

## 五、分析与思考

（1）同一个 DHCP 服务器中能否创建网段相同的两个作用域？

（2）DHCP 服务器中能否创建多个不同网段的作用域？

（3）DHCP 如何为客户机永久分配同一个 IP 地址？

（4）作用域选项设置与服务器选项设置有何区别？

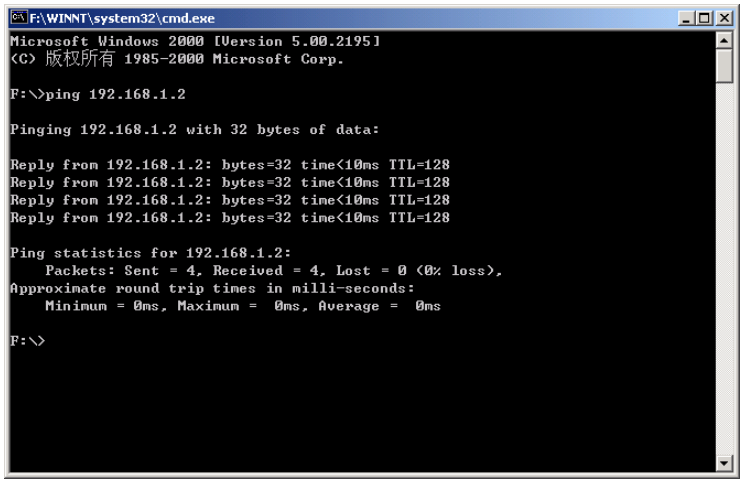



图 9-50　本地连接属性

# 实验 9　DNS 服务器的实现

**【实际应用背景描述】**

你是公司 IT 部门的员工，你们已对公司内部网站进行了发布，这时公司员工可以通过在 IE 浏览器中输入内部网站的 IP 地址实现对其的访问。但是员工反映，公司服务器太多，都是用 IP 地址访问，很容易混淆，能否用便于记忆的名字来代替。经技术部门协商，觉得将所有应用服务器通过域名来进行访问，使得大家容易记忆。

## 一、实验目的

（1）掌握 DNS 服务器的安装与配置。

（2）掌握 DNS 服务器的使用方法。

## 二、实验设备环境

（1）计算机两台。

（2）双绞线两根。

（3）交换机一台。

（4）操作系统环境：服务器　Windows Server 2003

客户机　Windows XP

## 三、实验前的准备

（1）DNS 的名称空间规划。在网络上开始使用 DNS 之前，请先确定 DNS 域名空间的规划。提出名称空间规划包括决定要如何使用 DNS 命名以及通过使用 DNS 要达到什么目的。

选择您的第一个 DNS 域名：完全合格域名（FQDN）

（2）确定唯一父 DNS 域名：jsj.net。

## 四、实验步骤

### 1．安装 DNS 服务器（注意：安装过程参照 DHCP 安装过程）

【步骤 1】打开 Windows 组件向导。

【步骤 2】在“组件”中，单击“网络服务”，然后单击“详细信息”按钮。

【步骤 3】在“网络服务的子组件”中，选择“域名系统（DNS）”复选框，然后单击“确定”按钮，再单击“下一步”按钮。

【步骤 4】在“文件复制来源”中，输入 Windows 2000 分配文件的完整路径，然后单击“确定”按钮。所需的文件被复制到硬盘上，重新启动系统后就可以使用服务器软件了。

### 2．配置新的 DNS 服务器

【步骤 1】打开 DNS 控制台窗口，如图 9-51 所示。

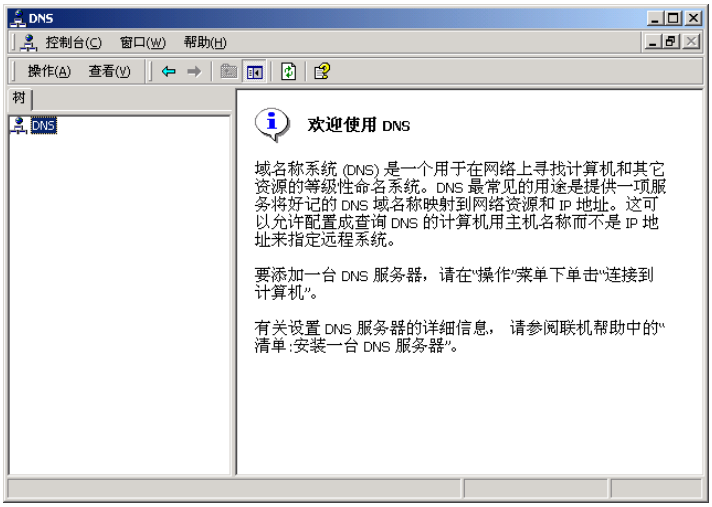



图 9-51　DNS 控制台窗口

【步骤 2】右击 DNS 图标，在快捷式菜单中选中“添加服务器”，添加需要配置 DNS 服务的计算机，如图 9-52、图 9-53 所示。

【步骤 3】新建区域：选中“正向搜索区域”项，如图 9-54 所示，再右击“正向搜索区域”，选择“新建区域”，打开新建区域向导对话框，如图 9-55 所示。

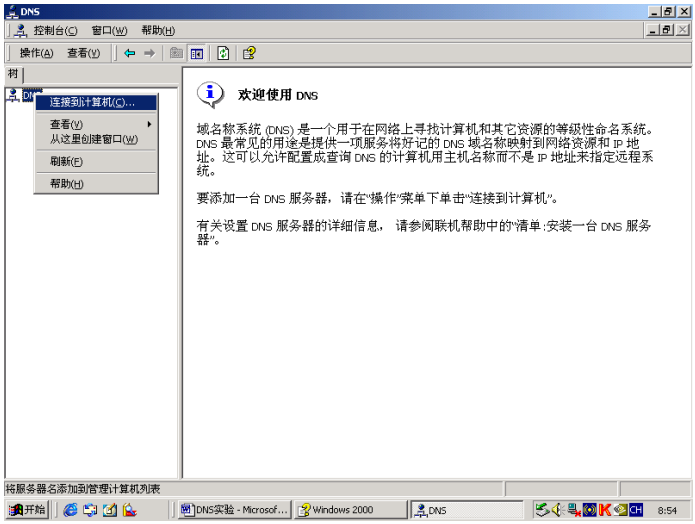



图 9-52　添加 DNS 服务器

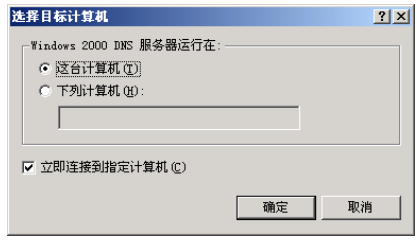



图 9-53　添加 DNS 服务器

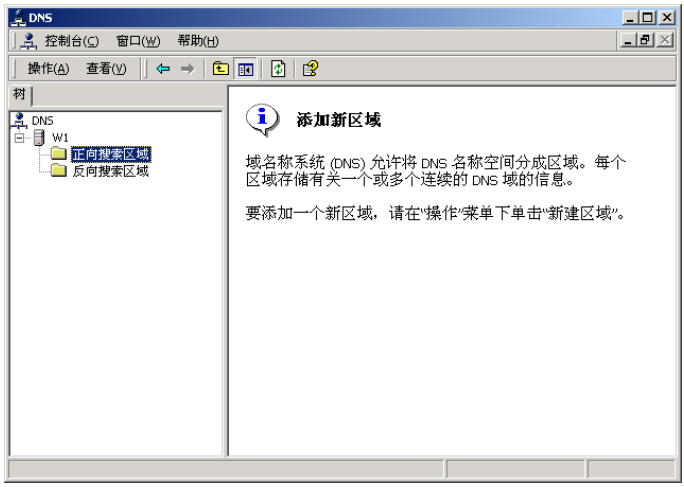



图 9-54　DNS 服务器控制台

【步骤 4】在随后打开的新建区域向导的“欢迎使用新建区域向导”对话框中，单击“下一步”按钮，打开“区域类型”对话框，如图 9-56 所示。


图 9-55　“新建区域向导”对话框

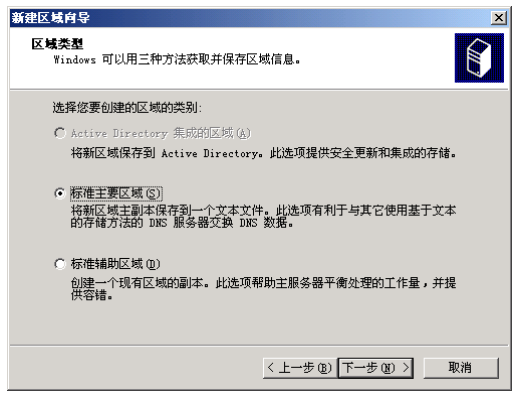



图 9-56　“区域类型”对话框

**注意**：如果这是网络中的第一台 DNS 服务器，则应选择“标准主要区域”选项或 Active Driectory 集成的区域，如果还没有创建活动目录，“Active Driectory 集成的区域”选项不可选。

**【步骤 5】**在此选择“标准主要区域”选项，单击“下一步”按钮，进入“区域名”对话框。例如，输入 jsj.net，如图 9-57 所示。

**【步骤 6】**单击“下一步”按钮，进入“区域文件”设置对话框，如图 9-58 所示。

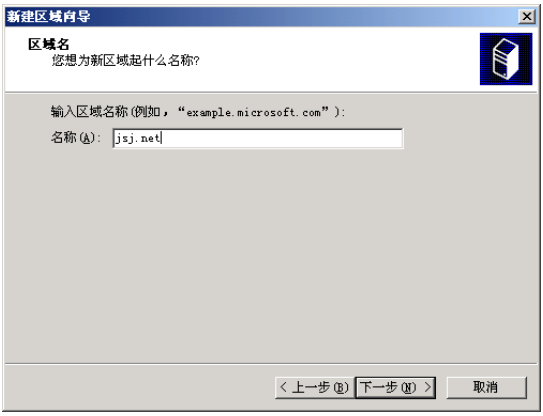



图 9-57　“区域名”对话框

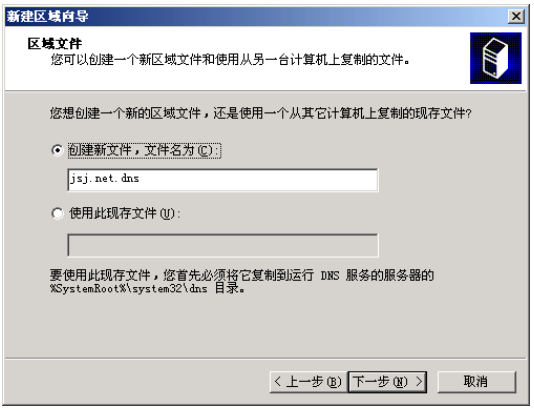



图 9-58　“区域文件”对话框

**【步骤 7】**保持默认设置不变，单击“下一步”按钮，将出现“正在完成新建区域向导”对话框，单击“完成”按钮，结束新建一个区域的工作。

**【步骤 8】**当 DNS 区域建好后，选中区域名，再右击该区域名，选择“新建主机”，如图 9-59 所示。

**【步骤 9】**在随后打开的“新建主机”对话框中，在名称输入一个主机名，这个主机名可根据需要随意取，不一定是真正的计算机名。在“IP 地址”栏中，输入对应主机的 IP 地址，如图 9-60 所示。

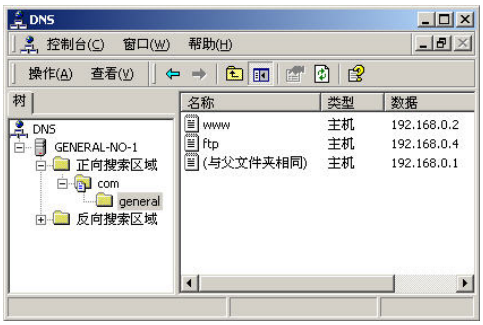



图 9-59　选中区域名

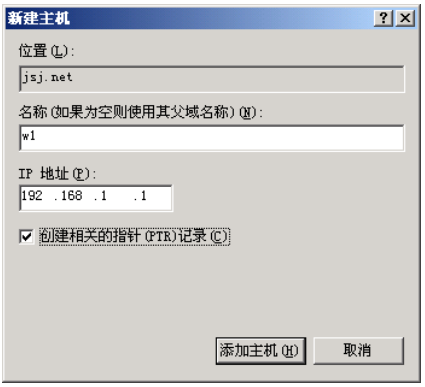



图 9-60　“新建主机”对话框

**【步骤 10】**单击“添加主机”按钮，将出现创建成功的对话框，如图 9-61 所示。

**【步骤 11】**添加其他主机，如图 9-62 所示。

3．测试验证 DNS

【步骤 1】DNS 服务器配置完成后，在客户端的 TCP/IP 属性对话框中，要设置 DNS 服务器的 IP 地址，或利用 DHCP 服务器分配 DNS 服务器的 IP 地址。

【步骤 2】在命令提示符下输入 ping<完整的域名>命令，以测试 DNS 服务是否生效。例如，在客户机设定 DNS 服务器的 IP 地址为：192.168.1.1，使用命令：

```
PING W1.JSJ.NET -T
PING W2.JSJ.NET -T
```


图 9-61　完成新建主机对话框

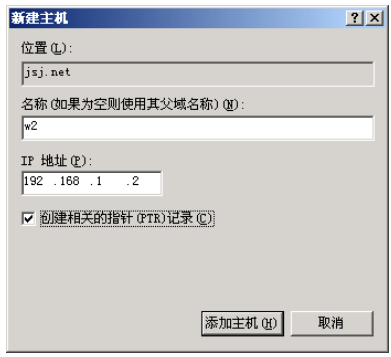



图 9-62　添加其他主机对话框

## 五、分析与思考题

（1）DNS 的命令格式是什么？
（2）一般的完整域名分为几个级别？
（3）正向搜索与反向搜索的区别是什么？
（4）如何配置 DNS 的动态更新？

# 实验 10　网线端接、跳线制作和测试实验

【实际应用背景描述】

某新建写字楼，前期的土建及装潢工作基本结束，并且已经开始招租，部分公司及企业开始准备入住办公，现要根据用户的需求完成水平干线子系统的设计和安装工作。

## 一、实验目的

（1）通过本实验掌握网络跳线的制作和压接线原理。
（2）掌握网络跳线的压接线方法和技巧。
（3）掌握网络线的色谱、剥线方法、预留长度和压接顺序。
（4）掌握网络线压接常用工具和操作技巧。

## 二、实验要求

（1）完成网络线的两端剥线。不允许损伤线缆铜芯，长度合适。
（2）完成 2 根网络跳线的制作实验，共计压接 4 个 RJ-45 水晶头。
（3）要求压接方法正确，达到 4 次压接，每次成功，压接线序检测正确。

## 三、实验设备、材料和工具

（1）端接试验台。
（2）网线 2 根，每根长度 500 毫米。
（3）RJ-45 水晶头 4 个，护套 4 个。
（4）网络压线钳 1 把，用于裁剪和压接 RJ-45 水晶头。
（5）钢卷尺 1 个，测量网线长度。

## 四、实验步骤

（1）打开网络实验台电源开关。观察电源指示灯是否正常。
（2）准备好实验工具。
（3）领取实验材料包，取出 2 根网线，每根长度为 500mm，RJ-45 水晶头 4 个，护套 4 个。
（4）制作 1 根 T568B 网络跳线的详细实验步骤和压线方法如下所述：

**【步骤 1】**利用压线钳或者斜口钳剪取所需要的双绞线长度，剪下后先将双绞线穿过护套。本实验使用材料包中已经备好的网线。

**【步骤 2】**利用剥线器将双绞线剥去外皮约 2cm（如图 9-64 所示），特别注意不能损伤线芯，并将 4 对线呈扇状拨开，顺时针从左到右依次为“白橙/橙”、“白蓝/蓝”、“白绿/绿”、“白棕/棕”。

**【步骤 3】**再将每一对线分开排齐，注意调整 2、3 对线的位置，使 8 条芯线按照 T568B 标准接线色谱依“白橙”、“橙”、“白绿”、“蓝”、“白蓝”、“绿”、“白棕”、“棕”的顺序，按照顺时针方向排列整齐。

**【步骤 4】**将 8 条线并拢后用压线钳剪齐，并留下约 14mm 的长度。

**【步骤 5】**将并拢的双绞线插入 RJ-45 接头中，注意“白橙”线要对着 RJ-45 的第 1 引脚。

**【步骤 6】**将 RJ-45 接头放入压接槽，一边将线往接头前端顶住，一边用力将压线钳夹紧。压紧接头后将压线钳松开并取出 RJ-45 接头即可。注意压过的 RJ-45 接头，其 8 只金属引脚一定要比未压过的低，这样才能顺利嵌入芯线中。抽出接头后，再把护套推往接头方向，套住接头，就算完成单边接头的压接。

**【步骤 7】**重复步骤 1～6，压好另一端的 RJ-45 接头，这条电缆就可以使用了。

**【步骤 8】**将做好的跳线两端的 RJ-45 水晶头分别插入网络跳线测试仪 RJ-45 接口中（如

图 9-65 跳线测试），听到“咔”的一声，就说明顺利完成了网线与测试口的连接，这时对应的 8 组指示灯依次闪烁。

图 9-63　网线制作


图 9-64　跳线测试

（5）网络跳线测试仪+RJ-45 配线架+110 通信跳线架组合压接线和测试实验。原理如图 9-66 所示。

**【步骤 1】**裁剪 1 根网线遵照 T568B 标准压接两端，制作成直通线。一端插入网络跳线测试仪，另一端接到 RJ-45 配线架的某个模块的 RJ-45 接口上。

**【步骤 2】**裁剪一根网线一端压接网络配线架模块，另一端压接到 110 通信跳线架下排接口。

**【步骤 3】**裁剪一根网线一端压接到 110 通信跳线架下排模块，另一端制作 1 个 RJ-45 水晶头，插入网络跳线测试仪。3 个步骤完成后，经过了 6 次压接，形成 1 个电气回路，对应的指示灯显示电气连接性能和线序状态。

**【步骤 4】**检查压接的正确性。如果压接正确时，对应的指示灯亮；如果压接不正确或者没有实现电气连接时，对应的指示灯不亮；如果压接线序不正确或者错位时，对应错位的指示灯亮显示。

## 五、实验报告

（1）写出 T568A、T568B 色谱等网络跳线 8 芯色谱和压接线顺序。
（2）写出网络跳线压接线的原理。
（3）总结出网络跳线压接线的方法和注意事项。

## 六、实验相关说明

（1）FLUKE 网络测试仪。
① 测试线缆类型：
- 屏蔽和非屏蔽双绞线（STP 和 UTP）。

- TIA Cat 3、4、5、5E、6：100Ω。
- 金属膜屏蔽双绞线（FTP，ScTP）。
- 10Base-5 粗缆，10Base-2 细缆，光缆。
- 选用光缆选件可测试单模和多模光缆。

② 支持测试：测试项目由所选的网络或标准来决定。

近端串扰（NEXT）、远端的近端串扰（NEXT）、接线图（Wire Map）、特性阻抗（Characteristic Impedance）、长度（Length）、直流环路电阻（DC Loop Resistance）、传输时延（Propagation Delay）、时延偏离（Delay Skew）、回波损耗（Return Loss）、远端的 RL、衰减（Attenuation）、衰减串扰比（ACR）、远端的衰减串扰比（ACR）、综合衰减串扰比（Power Sum ACR）、远端的综合衰减串扰比（PSACR）、等效远端串扰（ELFEXT），远端的等效远端串扰（ELFEXT）、综合等效远端串扰（PSELFEXT）、远端的综合等效远端串扰（PSELFEXT）、综合的近端串扰（PS NEXT）、远端的综合近端串扰（PSNEXT）。

③ 局域网流量：

- 监视器通过声音指示流量。
- 通过 RJ-45 插座监测 10Base-T 以太网流量。
- 通过 RJ-45 插座监测 100Base-TX 以太网流量。
- 通过 RJ-45 插座自动识别 10Base-T 和 100Base-TX。
- 可使 10Base-T，10/100Base-TX 或 100Base-TX 的 Hub 端口的链路指示灯闪亮。

（2）五类线网线测试报告。

如图 9-67 所示为用 FLUKE 网络测试仪检测的××学院图书馆 1 个点的网络布线报告：

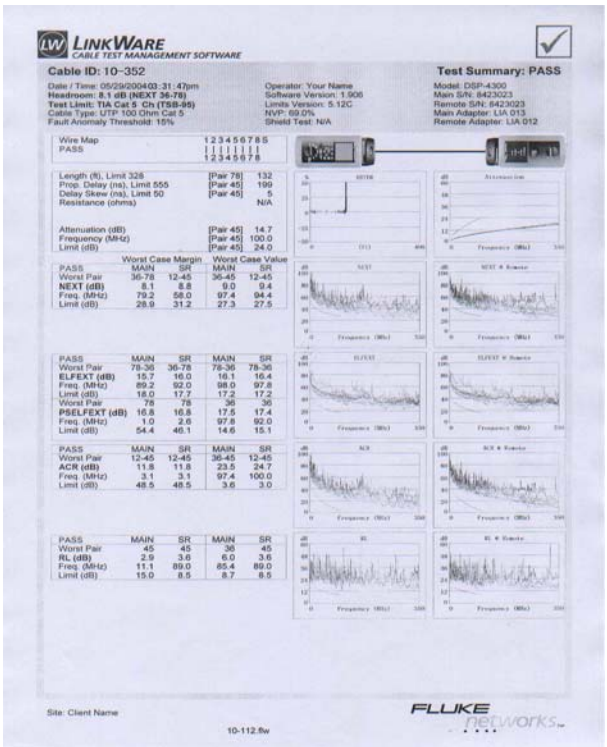



图 9-67　网络布线报告

（3）光缆测试报告。

表 9-2　××学院光纤测试报告

| 路　　由 | 光缆类型 | 色　　谱 | 测前值（DB） | 测后值（DB） | 单芯损耗（DB） |
|---|---|---|---|---|---|
| 网络中心——生活区 | 单模 | 红 | 14.30 | 14.90 | 0.60 |
| | | 绿 | 14.30 | 14.85 | 0.55 |
| | | 紫 | 14.30 | 14.85 | 0.55 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 棕 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.88 | 0.58 |
| 网络中心——综合区 | 多模 | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 棕 | 14.30 | 14.87 | 0.57 |
| | | 黑 | 14.30 | 14.86 | 0.56 |
| | | 本 | 14.30 | 14.90 | 0.60 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.85 | 0.55 |
| | | 蓝 | 14.30 | 14.90 | 1.60 |
| | | 本 | 14.30 | 14.85 | 0.55 |
| | | 蓝 | 14.30 | 14.85 | 0.55 |
| | | 本 | 14.30 | 14.90 | 0.60 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.88 | 0.58 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.87 | 0.57 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.86 | 0.56 |
| | | 红 | 14.30 | 14.90 | 0.56 |
| | | 本 | 14.30 | 14.88 | 0.58 |
| | | 绿 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.87 | 0.57 |
| | | 蓝 | 14.30 | 14.90 | 0.60 |
| | | 本 | 14.30 | 14.90 | 0.60 |

注：1．测试仪器：光功率计。

2．测试波长：多模：850NM。

单模：1 310NM。

3．测试人：×××。

（4）常用网络跳线产品，如图 9-68 所示。

（5）便携式网线测试仪。

（6）该系列网络测试仪通过自动扫描电缆专用于快速测试 10Base-T。

（7）(UTP/STP)-AT&T258A, TIA568A/B 以及 USOC4/6/8 模块化电缆的连接性线序及定位，

通过附带的远程终结器（该测试器）无论在电缆安装前后，都能测试电缆，如图 9-69 所示。


图 9-68　常用网络跳线产品

图 9-69　便携式网线测试仪

# 实验 11　网络管理工具的使用

**【实际应用背景描述】**

你是某公司的网络管理员，当遇到网络故障后，你能够灵活地使用网络管理工具，将网络故障轻松排除。同时，洞察网络潜在的各种威胁及时发现故障苗头并积极采取应对措施，将故障消灭于萌芽状态。

## 一、实验目的

（1）了解以太网工作原理，了解网卡的工作模式，理解网络嗅探的原理。

（2）使用 Ethereal 软件进行局域网流量捕获，深入理解 TCP/IP 协议的工作原理和过程。

## 二、实验设备环境

安装 Ethereal 软件的普通联网计算机。

## 三、实验内容

（1）安装和使用 Ethereal 软件进行局域网流量捕获。

（2）分析捕获的数据，理解捕获的数据包的类型和格式，学习利用捕获结果发现网络内的不良信息和病毒或木马的特征包。

## 四、实验注意事项

（1）注意防火墙软件配置对 Ethereal 结果的影响，必要时要关闭防火墙服务。

（2）以组为单位，分工协作，捕获并分析 ping 程序的 ICMP 数据包及访问简单网页的

HTTP 数据包，分析其格式和 TCP 连接过程。

## 五、实验相关内容

网络嗅探原理：以太网的数据传输是基于“共享”原理的：所有的同一本地网范围内的计算机共同接收到相同的数据包。这意味着计算机直接的通信都是透明可见的。正是因为这样的原因，以太网卡都构造了硬件的“过滤器”来忽略掉一切和自己无关的网络信息（事实上是忽略掉了与自身 MAC 地址不符合的信息）。而网络嗅探程序利用了这个特点，它主动的关闭了过滤器，也就是设置了网卡“混杂模式”，此时，嗅探程序就能够接收到整个以太网内的网络数据信息，并加以分析。通过对得到的数据包进行一定的分析，网络嗅探程序可能得到许多有价值的信息，包括机密数据、账户密码等，得到有用信息的难易程度，取决于许多因素，如数据包的类型、加密程度等。

Ethereal 是免费的网络协议检测程序，可以用来监视所有在网络上被传送的包，并分析其内容，支持 UNIX，Windows 系统。用户经由程序抓取运行的网站的相关资讯，包括每一封包流向及其内容、资讯可依操作系统语系看出，方便查看、监控 TCP session 动态等。它通常被用来检查网络工作情况，或是用来发现网络程序的 bugs。目前 Ethereal 提供了对 TCP、UDP、SMB、Telnet 和 FTP 等常用协议的支持。它在很多情况下可以代替价格昂贵的 Sniffer。

## 六、实验步骤

### 1．Ethereal 的安装

Ethereal 是一个图形用户接口（GUI）的网络嗅探器，由于 Ethereal 需要 WinPcap 库，所以先安装 WinPcap_2_3.exe，再安装 Ethereal.exe。

### 2．Ethereal 抓包过程

**【步骤 1】**双击启动桌面上的 Ethereal 图标，Ethereal 工具的主界面非常简洁，整个窗口被分成 3 个部分：最上面的窗口为数据报文列表窗口，用来显示截获的每个数据报文的总结性信息；中间窗口为协议树窗口，用来显示选定的数据报文的协议信息；下边窗口是以十六进制形式表示的数据报文内容窗口，用来显示数据报文在物理层上传输时的形式。

**【步骤 2】**在主界面中，单击“Filter”按钮，打开过滤器的设置界面，可以根据需要选取或直接输入过滤命令，并支持 and/or 的功能连接。单击“OK”按钮配置结束。

**【步骤 3】**单击菜单“capture|interface”查看可以进行监听的端口，如图 9-70 所示。

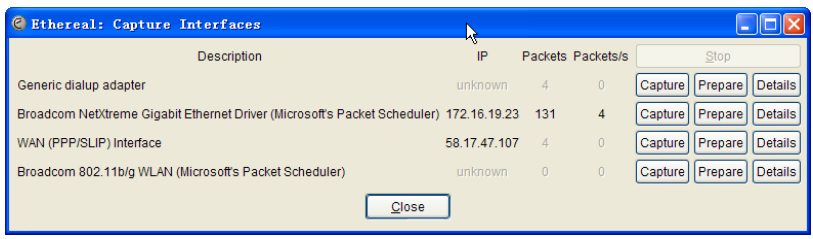



图 9-70 “Capture Interface”窗口

【步骤 4】单击图 9-70 中需要监听接口的“Prepare”，可以进行监听接口的选择和设定，如图 9-71 所示。（单击“Start”按钮即可在“Interface”栏选定的接口上进行嗅探、监听。）然后单击“Cancel”回到“Interface”界面。

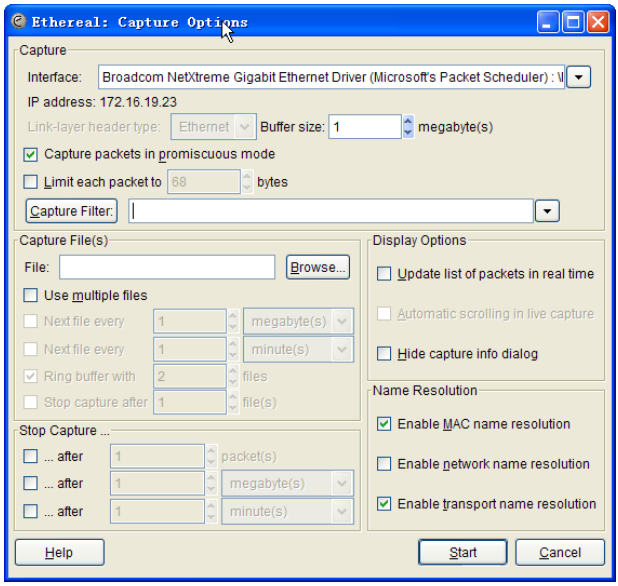



图 9-71　Capture Options 窗口

【步骤 5】在“Interface”界面中单击需要监听接口的“Capture”按钮即可进入网络嗅探状态，如图 9-72 所示。

【步骤 6】当有需要的数据包出现或监听一段时间后，单击“stop”按钮，结束监听并自动进入协议分析界面，如图 9-73 所示。

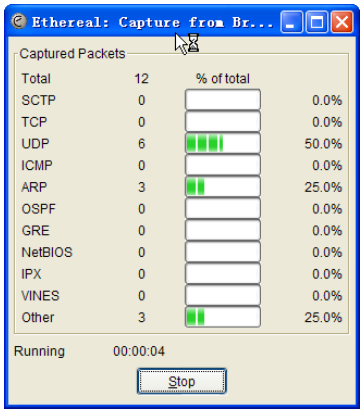



图 9-72　Capture 窗口

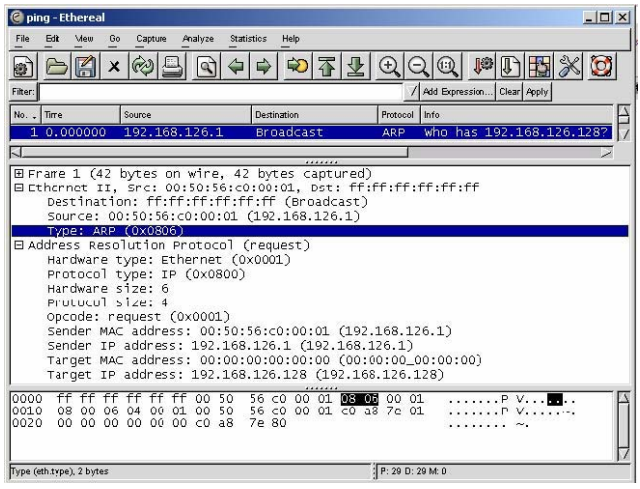



图 9-73　用 Ethereal 分析数据包内容

数据报文列表窗口显示了发送数据报文时，数据报文的源地址、目的地址、协议类型、数据信息等信息。协议树窗口显示数据报文更详细的信息，如 MAC 地址（Ethereal Ⅱ）、IP 地址（Internet Protocol）、TCP 端口号（Transmission Control Protocol），以及协议的具体内容。

在数据报文列表窗口上单击一个数据报文，然后在协议树窗口上查看这个报文的内容，如果需要的话，还可以对数据报文内容窗口的十六进制数据进行分析。

## 七、实验总结

网络协议分析技术主要用来帮助网络管理员对网络进行管理。通过网络协议分析技术，网络管理员可以了解目前网络中正在应用的协议种类，每种协议所占的比例，及哪些设备应用哪些协议进行通信；同时可以分析协议应用的合理性与有效性，从而合理地选择协议，节约有限的网络宽带，提高网络传输效率；另外，可以诊断出大量的不可见模糊问题，为管理员管理网络区域提供了非常宝贵的信息。